ATTUALITÀ

La Sicurezza Informatica tallone d'Achille della Nuova Sanità

di **Fondazione AIDR** · 11 ottobre 2021, 10:28

Giancarlo De Leo, Consulente in Editoria Medico-Scientifica e Sanità Digitale, Socio e Segretario dell' Osservatorio Sanità Digitale dell'Associazione Italian Digital Revolution (AIDR)

Negli ultimi anni l'aumento dei bisogni sanitari e l'avanzamento della tecnologia, hanno determinato per il settore sanitario la necessità di adattare i modelli tradizionali alle innovazioni tecnologiche, creando un nuovo modo di gestire la salute.

I sistemi sanitari sono diventati più digitali e interconnessi e consentono un più veloce e facile accesso ai servizi sanitari offerti.

Durante l'attuale situazione di emergenza sanitaria generata dalla pandemia da Covid-19 l'adozione di nuove tecnologie in ambito in Sanità, che non può prescindere dall'Health Technology Assessment (HTA: un approccio che si propone di valutare l'introduzione e la dismissione di tecnologie sanitarie in un'ottica multidisciplinare, per supportare chi ha potere decisionale in ambito sanitario), si è dimostrata efficace nel migliorare l'accesso alle cure e alla qualità di vita dei cittadini-pazienti, ma soprattutto, ha determinato un'accelerazione del fenomeno digitale che ha trovato il Sistema Sanitario Nazionale gravemente sotto pressione, dovendo rispondere ad una sempre maggior richiesta di assistenza sanitaria e, al tempo stesso, garantire il distanziamento sociale per impedire la diffusione del contagio.

La digitalizzazione della sanità rappresenta una grande sfida per il futuro e un'opportunità per colmare il divario sempre più crescente tra il progressivo invecchiamento della popolazione e la mancanza di risorse disponibili.

In questo scenario, la sicurezza informatica riveste un ruolo di primo piano: nel settore salute gli attacchi informatici si intensificano ogni giorno sempre di più e sono particolarmente preoccupanti, in quanto possono minacciare la sicurezza dei dati e delle informazioni sanitarie

oltre alla salute dei pazienti.

A tal proposito sono stati rilevati, tra l'altro, numerosi attacchi contro organizzazioni sanitarie e laboratori di ricerche attivi nella ricerca per il contrasto al Coronavirus.

Lo strumento offensivo utilizzato è sovente il "ransomware", un software che si appropria dei dati delle strutture sanitarie e delle informazioni personali dei pazienti tenendoli bloccati fino a quando i soggetti che lo hanno creato non ricevono in pagamento il riscatto richiesto.

Dal whitepaper "Capire il rischio cyber- Il nuovo orizzonte in sanità", che raccogliendo le risposte di 68 professionisti sanitari (Risk Manager, Responsabili Qualità, Data Protection Officer, Responsabili della sicurezza informatica e dell'Ingegneria Clinica, nonché Referenti della Direzione Sanitaria e Generale) operanti in strutture distribuite su 14 Regioni italiane, analizza la preparazione e la consapevolezza della Sanità italiana per far fronte alla minaccia cyber (*con il termine cybersecurity si devono intendere quegli aspetti di sicurezza delle informazioni attuate attraverso l'uso di strumenti tecnologici. La sicurezza delle informazioni è prima di tutto un approccio completo alla gestione della sicurezza, di cui la cybersecurity è solo un sottoinsieme*) ciò che emerge é che la minaccia hacker non è sottostimata.

Si conferma il trend di attacchi informatici ad ospedali e centri medici italiani.

Il 24% delle strutture sanitarie del nostro Paese ha infatti riferito di aver subìto attacchi informatici nel 2020, dei quali l'11% è stato costituito da ransomware e il 33% da accessi abusivi ai dati.

Stando alla ricerca, infatti, il 59% delle strutture percepisce il tema cyber risk in sanità come una priorità che impatta su prestazioni erogate e modelli organizzativi interni. Un ulteriore 31% ha valutato il tema come parzialmente prioritario. Ciononostante gli analisti rilevano che sono ancora poco frequenti le misure adottate dalle strutture per prevenire e gestire il rischio cyber: mappature, analisi dei rischi e test di vulnerabilità figurano solo in un terzo del totale.

Ad avvalorare uno scenario piuttosto preoccupante è anche l'Agenzia europea per la sicurezza informatica, ENISA, secondo cui gli attacchi alle catene di approvvigionamento europee si quadruplicheranno nel corso del 2021, rispetto allo scorso anno (https://www.aidr.it/cyber-resilience-act-e-polo-informativo-europeo-sulla-difesa-cibernetica/).

Per far fronte al problema della sicurezza informatica il D.L. n. 82 del 14 giugno 2021, recante "Disposizioni urgenti in materia di cyber sicurezza, definizione dell'architettura nazionale di cyber sicurezza e istituzione dell'Agenzia per la cyber sicurezza nazionale" ha istituito, all'art.5, l'

Agenzia per la cyber sicurezza nazionale (https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG) convertito dalla Legge n. 109 del 4 agosto 2021(https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/sg).

La legge 109/2021, che definisce l'Architettura Nazionale di Cybersicurezza, introduce diverse novità in materia e istituisce:

- L'Agenzia Nazionale per la Cybersecurity;
- Il Comitato interministeriale per la cybersicurezza;
- Il Nucleo per la cybersicurezza

Ma ora, nel mese europeo della cybersicurezza che si tiene ogni anno ad ottobre, quali possibili suggerimenti?

1) Puntare su Informazione e Formazione
Una corretta e puntuale informazione sui possibili rischi e un'adeguata formazione sui temi della cybersecurity costituisce la prima linea di difesa contro il cybercrime che, nella maggior parte dei casi, è favorito proprio dall'errore o dalla negligenza delle persone. Un dipendente non formato potrebbe, ad esempio, aprire email sospette o non proteggere adeguatamente informazioni sensibili adottando comportamenti non conformi alla sicurezza.

2) Adottare soluzioni di Email Security Virtual Appliance per la Posta elettronica
La posta elettronica è il principale mezzo di comunicazione aziendale. Si stima che attualmente vengano inviate oltre 300 bilioni di email al giorno. Non c'è quindi da meravigliarsi del fatto che l'email sia lo strumento preferito dagli hackers per veicolare gli attacchi, di cui ne esistono tantissime varianti: malware, botnet, whaling, phishing. Meno pericoloso, ma senza dubbio fastidioso, è lo spam mediante il quale vengono inviate pubblicità massive che rallentano e sviano l'attività lavorativa dei dipendenti.

3) Prendere in considerazione soluzioni di Adaptive Multi-factor Authentication per Username e Password
I tradizionali username e password non sono più sufficienti per autenticare gli utenti. Ogni giorno si racconta di nuove storie di furti di identità ad opera degli hacker a vari livelli di gravità. Credenziali deboli o credenziali rubate sono le armi preferite utilizzate dagli hacker e rappresentano circa il 76% di tutte le intrusioni di rete.

4) Utilizzare la tecnologia di virtualizzazione dello storage
La tecnologia di virtualizzazione dello storage trasforma il normale spazio su disco in un "pool" di

storage gestito centralmente, sempre disponibile e più veloce: riduce i colli di bottiglia di I / O e le perdite di fatturato, migliora le prestazioni, diminuisce i costi ed i rischi. Questo software, completamente agnostico all'hardware, colma il divario tra le esigenze aziendali di avere risposte in tempo reale e la necessità di sfruttare al massimo le risorse IT attuali e future, con un forte orientamento all'ottimizzazione del carico di lavoro.

5) Lavorare su uno spazio di lavoro unificato

Uno spazio di lavoro unificato che offra un accesso altamente sicuro e controllato ai file e alle applicazioni legacy, Web e SaaS in uno spazio di lavoro basato su browser, accessibile tramite qualsiasi browser, su qualsiasi dispositivo. Ma solo un sano ed onesto buon senso permetterà quindi di non incorrere in danni irreparabili per i cittadini del Sistema Sanitario Nazionale.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/10/11/la-sicurezza-informatica-tallone-dachille-della-nuova-sanita/

© 2026 Istituzioni24