20/12/2021

difesaonline.it

Argomento: Exprivia: si parla di noi

EAV: € 845
Utenti unici: 8.400

https://www.difesaonline.it/evidenza/cyber/cybersecurity-e-sanit%C3%A0

CYBERSECURITY E SANITÀ

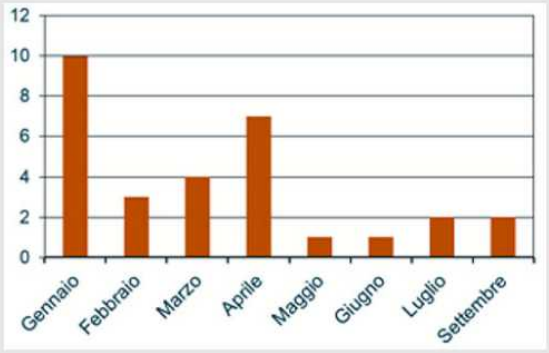
20/12/21 - Gli attacchi Cyber ad infrastrutture sanitarie si stanno intensificando in numero e in qualità e sempre più frequentemente hanno successo portando in primo piano l'esigenza di migliorare le strategie di prevenzione e di risposta. Si descriveranno sinteticamente le principali aree tecnologiche ed organizzative sulle quali è necessario porre immediatamente attenzione e fare azioni anche a livello di budget.

La strumentazione medicale è ormai pervasa dal digitale ed è quindi soggetta a sempre più pericolosi attacchi per questo, deve essere opportunamente protetta. In ambito sanitario la maggioranza dei dati trattati è classificabile come sensibile e viene utilizzato in modalità differenti da diverse tipologie di utenza, e per questo, conseguentemente, deve essere gestito e protetto con azioni preventive e protettive. Di seguito, si affronterà anche il tema dei servizi gestiti di sicurezza che possono essere risolutivi nell'aiutare le organizzazioni sanitarie ad incrementare la propria efficacia nella prevenzione e risposta ai rischi di Cybersecurity, vediamo infatti una grossa valenza strategica in questo approccio poiché permettono di usufruire di alte competenze, difficilmente ottenibili senza impatti eccessivamente onerosi per le strutture stesse.

Evoluzione e quadro attuale del rischio Cyber

Nel 2019 una donna dell'Alabama ha indetto causa ad un ospedale locale per non averla informata del fatto che il giorno prima lo stesso avesse ricevuto un attacco informatico. Secondo la donna, durante il parto il personale sanitario non avrebbe avuto la disponibilità piena degli strumenti digitali necessari durante l'intervento e questo avrebbe causato un danno prima e successivamente la morte della neonata. L'ospedale ha dichiarato che l'attacco era avvenuto il giorno prima del parto. L'accusa, sostenne che la donna, se fosse stata informata dell'attacco, avrebbe potuto modificare la sua decisione, scegliendo un'altra struttura.

Altro importante episodio, avvenuto a settembre 2020, vede la morte di una donna a causa di un attacco informatico in Germania. L'attacco, di tipo ransomware, ha reso indisponibili i servizi digitali per la accoglienza e pertanto la donna è stata costretta ad essere trasportata in un altro ospedale. Il ritardo ne ha causato la morte.



In Italia lo stato dell'arte, non sembra essere molto più favorevole anche se ad oggi non si sono registrati casi di specie.

Precisamente, nel corso del 2021 ci sono stati ben 30 incidenti, attacchi e violazioni privacy che hanno interessato il mondo della sanità, come riportato graficamente dal report 3Q 2021 dell'*Osservatorio Exprivia Cybersecurity*. Ad inizio anno sono stati registrati numerosi attacchi mentre in misura minore gli incidenti (attacchi andati a buon fine).

Nonostante un dato positivo in termini di sicurezza, le buone notizie finiscono qui. Infatti, nel corso del 2Q 2021 e del 3Q 2021 la forbice tra attacchi ed incidenti si è ristretta drasticamente.

Analizzando i dati nel loro dettaglio, questo aumento degli incidenti di sicurezza indica inevitabilmente una maggiore attenzione dei cybercriminali nello sferrare attacchi sempre più sofisticati e in secondo luogo una

CyberSecurity e Sanità

Gli attacchi Cyber ad infrastrutture sanitarie si stanno intensificando in numero e in qualità e sempre più frequentemente hanno successo portando in primo piano l'esigenza di migliorare le strategie di prevenzione e di risposta. Si descriveranno sinteticamente le principali aree tecnologiche ed organizzative sulle quali è necessario porre immediatamente attenzione e fare azioni anche a livello di budget.

La strumentazione medicale è ormai pervasa dal digitale ed è quindi soggetta a sempre più pericolosi attacchi per questo, deve essere opportunamente protetta. In ambito sanitario la maggioranza dei dati trattati è classificabile come sensibile e viene utilizzato in modalità differenti da diverse tipologie di utenza, e per questo, conseguentemente, deve essere gestito e protetto con azioni preventive e protettive. Di seguito, si affronterà anche il tema dei servizi gestiti di sicurezza che possono essere risolutivi nell'aiutare le organizzazioni sanitarie ad incrementare la propria efficacia nella prevenzione e risposta ai rischi di Cybersecurity, vediamo infatti una grossa valenza strategica in questo approccio poiché permettono di usufruire di alte competenze, difficilmente ottenibili senza impatti eccessivamente onerosi per le strutture stesse.

Evoluzione e quadro attuale del rischio Cyber

Nel 2019 una donna dell'Alabama ha indetto causa ad un ospedale locale per non averla informata del fatto che il giorno prima lo stesso avesse ricevuto un attacco informatico. Secondo la donna, durante il parto il personale sanitario non avrebbe avuto la disponibilità piena degli strumenti digitali necessari durante l'intervento e questo avrebbe causato un danno prima e successivamente la morte della neonata. L'ospedale ha dichiarato che l'attacco era avvenuto il giorno prima del parto. L'accusa, sostenne che la donna, se fosse stata informata dell'attacco, avrebbe potuto modificare la sua decisione, scegliendo un'altra struttura.

Altro importante episodio, avvenuto a settembre 2020, vede la morte di una donna a causa di un attacco informatico in Germania. L'attacco, di tipo ransomware, ha reso indisponibili i servizi digitali per la accoglienza e pertanto la donna è stata costretta ad essere trasportata in un altro ospedale. Il ritardo ne ha causato la morte.

In Italia lo stato dell'arte, non sembra essere molto più favorevole anche se ad oggi non si sono registrati casi di specie.

Precisamente, nel corso del 2021 ci sono stati ben 30 incidenti, attacchi e violazioni privacy che hanno interessato il mondo della sanità, come riportato graficamente dal report 3Q 2021 dell'Osservatorio Exprivia Cybersecurity. Ad inizio anno sono stati registrati numerosi attacchi mentre in misura minore gli incidenti (attacchi andati a buon fine).

Nonostante un dato positivo in termini di sicurezza, le buone notizie finiscono qui. Infatti, nel corso del 2Q 2021 e del 3Q 2021 la forbice tra attacchi ed incidenti si è ristretta drasticamente.

Analizzando i dati nel loro dettaglio, questo aumento degli incidenti di sicurezza indica

inevitabilmente una maggiore attenzione dei cybercriminali nello sferrare attacchi sempre più sofisticati e in secondo luogo una minore attenzione da parte degli utenti e degli operatori che diventano vittime.

Oltre al cybercrime, una notevole importanza la assumono le violazioni della privacy segnalate dal Garante. Sono ben 12 le segnalazioni nella prima parte dell'anno e quest'aspetto che non si può sicuramente ricondurre ad attività criminali, suggerisce forti riflessioni dal punto di vista organizzativo e strutturale.

Ultima considerazione sui dati in Italia raccolti ed analizzati dall'Osservatorio di Cybersecurity di Exprivia, riguarda le tecniche di attacco utilizzate verso le strutture e i sistemi sanitari; la fanno da padrona le tecniche che prevedono lo sfruttamento delle vulnerabilità note ed a seguire le campagne di phishing con esiti fatali.

Se da un lato il benessere di una comunità non può prescindere dalla necessità di investire in sanità rendendo la stessa sempre più efficace dal punto di vista organizzativo, utilizzando al meglio le tecnologie che il mercato mette a disposizione, dall'altra è impensabile che tali benefici possano non passare attraverso un aggressivo percorso di digitalizzazione che sia accompagnato da una continua valutazione del rischio informatico ad esso associato.

Maggiore sarà l'utilizzo di servizi digitali, maggiori saranno le esposizioni di questi servizi ad attacchi e conseguentemente a incidenti.

Alla luce dei dati in nostro possesso seguono pertanto le aree di maggiore attenzione e relativi suggerimenti.

Consapevolezza sui rischi relativi ad un attacco informatico

Malgrado gli attaccanti abbiano la possibilità di sfruttare tecniche estremamente sofisticate, spesso l'incidente è causato dal cadere vittima di tranelli perpetrati tramite campagne di phishing estremamente banali per addetti ai lavori, ma che potrebbero essere meno ovvi per il personale con mansioni e specializzazioni differenti. Nello specifico, il personale specializzato in IT è in minima percentuale rispetto a coloro che operano a diretto o indiretto contatto con il paziente (medici, infermieri...). Non dovrebbe sorprendere pertanto che il phishing rappresenti una notevole fetta delle metodologie di attacco usate nella sanità.

Necessario pertanto investire in programmi di consapevolezza. Il firewall umano è spesso la barriera più efficace contro il crimine informatico.

Verifica del grado di consapevolezza

Lo step successivo, dopo aver sensibilizzato e acquisito consapevolezza è investire nel controllare la qualità dell'approccio, dunque valutare come i vari programmi di awareness abbiano introdotto dei miglioramenti.

Certificazione

La certificazione delle competenze è una best practices dell'industria che non può essere ignorata neanche nel campo della sanità. Far conseguire a programmi di awareness delle certificazioni su piattaforme adeguate (ad esempio Open Badge 2.0) ne è una conseguenza.

Cyber-range

Per verificare quanto elevata sia la consapevolezza degli individui e quanto pronta sia l'organizzazione sanitaria a gestire un attacco informatico, è possibile fare delle simulazioni e osservare il comportamento della popolazione. Questa pratica, conosciuta come cyber-range, è comune negli ambienti IT ed in altre industrie che possono usare dei framework sviluppati ad hoc (ad esempio

TIBER-EU), ma che devono e possono essere adattati al mondo della sanità.

Aggiornamento dispositivi e zero-trust

Gran parte degli attacchi che hanno successo nel settore Healthcare sono riconducibili alle vulnerabilità conosciute e quindi sono incidenti evitabili. Questo non dovrebbe sorprendere in quanto in sanità il perimetro è estremamente esteso ed il controllo fisico è difficile da monitorare poiché sono spesso utilizzati dispositivi di informatica individuale. Avere una gestione unica della infrastruttura che identifichi e faccia rispettare delle policies, per la diversità dei servizi offerti, per la eterogeneità del personale che accede ai servizi, è estremamente difficile e complesso.

Dobbiamo aggiungere inoltre che la digitalizzazione implica una forte interconnessione di servizi e dispositivi e, pertanto, il malfunzionamento dell'uno potrebbe causare problemi ad un paziente apparentemente non coinvolto nell'incidente.

In Germania, la morte del paziente è una conseguenza dell'attacco al servizio di ricevimento dei pazienti, che apparentemente potrebbe sembrare non estremamente critico in quanto reversibile.

Protezione apparati digitali sanitari

L'attività sanitaria e più in generale la medicina, vede sempre più presenti strumenti elettronici sia a supporto della diagnostica, che della terapia e della gestione del malato. L'utilizzo di dispositivi intelligenti (IoT) ne sono una prova.

Questi strumenti, sempre più numerosi in ospedali e spesso affidati direttamente ai pazienti, offrono da un lato l'opportunità di migliorare qualitativamente e quantitativamente l'operato del personale sanitario, d'altro canto, purtroppo, espongono la struttura sanitaria ad attacchi di tipo informatico che possono essere estremamente pericolosi e creare danni ingenti a persone e cose.

Proprio i dispositivi IoT sono estremamente appetibili ai cybercriminali poiché utilizzabili come base di attacchi di tipo Distributed Denial of Service (DDoS). Non solo, sono frequenti casi in cui i malintenzionati hanno interrotto i servizi di interi reparti ospedalieri chiedendo uno o più riscatti (cd. double extrortion).

È quindi inevitabile e necessario iniziare a progettare le strutture informatiche e di rete in funzione di questi fattori di rischio e prevedere opportune strumentazioni di difesa. Adottare politiche di zero-trust utilizzando anche tecniche di micro-segmentazione delle reti è necessario per evitare che dispositivi non adeguatamente protetti possano entrare in contatto con persone e altri dispositivi che hanno diverse policies di sicurezza.

Privacy e protezione del dato

Quando si parla di cybersecurity si fa spesso riferimento alla possibilità che un servizio venga interrotto. Non possiamo però dimenticare che in Italia ci sono state violazioni di dati inerenti la privacy in quantità superiore agli incidenti di sicurezza nel mondo della sanità.

A questo si aggiunge il fatto che i criminali spesso sono interessati non tanto a interrompere il servizio, ma a rubare i dati (ultimamente si sono sviluppate anche tecniche di estorsione doppia in cui prima i dati vengono rubati e quindi il database criptato in modo da poter ricattare la vittima per ripristinare i dati, ma anche per restituire i dati).

Se il dato infatti è fondamentale alla esecuzione del servizio, nella sanità è estremamente critico ed appetibile sul mercato nero. Più in generale, i dati sono "critici" perché aiutano le macchine a far

vivere i pazienti, ma sono anche “sensibili”. Se da un lato il dato va protetto da possibili intromissioni malevole, dall’altro bisogna garantire un elevata tutela della privacy.

Per questo motivo si richiedono diversi livelli di protezione, quali l'adozione di opportune tecniche di crittografazione sia in conservazione che durante la trasmissione, una attenta profilazione degli utenti/sistemi e ruoli che vi possono accedere e infine un controllo continuo delle attività in grado di identificare atti fraudolenti sia provenienti da attori esterni che interni alla organizzazione.

Le peculiarità dei dati personali in ambito sanitario suggeriscono strategie di gestione particolari

I dati sanitari sono caratterizzati dall’essere oggetto di trattamento contemporaneo da almeno tre macro categorie di utenti e di servizi differenti al medesimo tempo:

Questi tre approcci convergenti sui medesimi dati in realtà non hanno sempre la necessità di accedere all'intero insieme di informazioni presente, né di farlo con identiche modalità.

Per esempio il trattamento a finalità scientifiche, probabilmente, non necessita mai di accedere ai dati personali di identità delle persone che invece sono essenziali alle altre tipologie di trattamento, viceversa i trattamenti gestionali e operativi, generalmente non hanno necessità di scendere in particolare dettaglio sugli aspetti medico analitici delle informazioni relative a una certa persona, ma più tipicamente si fermano a fattori di tipo quantitativo, quali numero e tipologie di esami differenti, indipendentemente dal risultato degli esami stessi.

Queste considerazioni suggeriscono di adottare fin da subito una strategia di protezione e accesso ai dati che tenga conto di queste differenze d'uso e che permetta una segmentazione efficiente ed efficace dei dati e dei loro livelli di accesso.

Per cui è opportuno che fin dalla fase di progettazione delle basi di dati si prevedano strategie di protezione classificata e granulare delle informazioni, proprio perché non tutti gli utilizzi necessitano dell'insieme di tutte le informazioni. Anche se questo può apparire in prima battuta più complesso rispetto ad una gestione monolitica della crittografazione, in realtà tenendo conto dell'intero ciclo di vita del dato e della necessità di controllo degli accessi, così non è perché singoli profili di accesso sono più semplici da proteggere ed espongono meno dati.

La segregazione preventiva e la granularità del mascheramento crittografico rappresentano un fattore importante nel progettare le proprie strategie di conservazione di protezione in funzione dei diversi utilizzi, esponendo meno informazioni in fase di utilizzo e semplificando poi tutta la parte di controllo e la protezione dei risultati delle elaborazioni.

Organizzazione della sicurezza in sanità

Le strutture sanitarie aspirano alla protezione ed al benessere dell'individuo, quindi si tratta prevalentemente di organizzazioni capillari e strutturate sul territorio. Questo implica che esse debbano essere tendenzialmente distribuite sul territorio ed agili.

Questa caratteristica, ovviamente, pone alcune sfide nel contesto della gestione della sicurezza cyber, principalmente perché le competenze e le strutture di sicurezza che sono necessarie per poter adempiere al ruolo e proteggere con la miglior efficacia possibile, sono difficilmente organizzabili su strutture territoriali di piccole e medie dimensioni, vuoi per una intrinseca carenza di competenze del comparto sicurezza attuale, ma anche e soprattutto per ovvie considerazioni di tipo

economico e organizzativo.
Si ritiene quindi opportuno valutare l'adozione di strategie organizzative che favoriscano la condivisione e la fruibilità di competenze altamente specialistiche più critiche per l'ambito Cyber in modo che possano essere condivise da più strutture con maggiore efficienza ed economia.
L'approccio basato su servizi gestiti è quindi da vedere con estremo interesse perché permette di avere accesso alle migliori competenze sui molti e diversi settori specifici dell'ambito sicurezza, quando e quanto necessario, senza accollarsi oneri economici eccessivi e senza obbligare le figure interne a percorsi formativi di eccessivo impegno in termini di conoscenze e competenze.
La Cyber Security è strutturalmente in continua evoluzione, con nuovi approcci e nuove strategie dovute all'adozione di nuove tecnologie. È impensabile che è una struttura agile come un ospedale possa essere messa in grado di dotarsi di tutte le competenze Cyber Security ormai irrinunciabili all'interno delle proprie strutture IT.
Fabiano Vincenzo Malerba (Exprivia Security Researcher)