Business Provider
COREUP

Perché gli hacker attaccano gli studi medici e le cliniche?

Piccola guida sull'importanza di proteggere i dati dei tuoi pazienti

Gli hacker prendono sempre più di mira gli **studi medici e dentistici** e le **cliniche private** perché sono una fonte importante di dati sensibili. Il motivo principale che spinge i criminali ad attaccare l'ambiente **healthcare** è che i **dati sanitari** sono facilmente rivendibili sul dark web con ricavi cospicui.

Inoltre, il settore sanitario nel nostro Paese investe ancora troppo poco nella **cybersecurity** presentando spesso vulnerabilità importanti che lo rendono più semplice da attaccare rispetto, ad esempio, al settore bancario.

Le minacce informatiche al settore sanitario:

La violazione dell'integrità dei dati medici è uno dei danni maggiori legato al rischio di modifica dei risultati dei test o dei trattamenti con gravi ripercussioni sulla salute delle persone. Un altro grande problema riguarda il rallentamento o il blocco delle prestazioni sanitarie in seguito a un attacco hacker: pensiamo a un ospedale sotto attacco che deve rimandare operazioni già pianificate. I rischi più ricorrenti nel settore healthcare sono:

1. **Violazione dei dati:** ·furto di dati sensibili sanitari (risultati di test medici, trattamenti, numeri di previdenza sociale, etc) per rivenderli sul dark web o per manometterli e/o furto di identità.
2. **Ransomware:** i cybercriminali criptano i dati dei pazienti e chiedono un riscatto per sbloccarli.
3. **Manomissione dei dispositivi medici:** la connessione alla rete di macchinari di monitoraggio, come quelli cardiaci, rende vulnerabile il loro funzionamento.

Questione di sicurezza (ma anche di reputazione)

Una riflessione: Quando si parla di salute entrano in gioco anche le emozioni e quel bisogno di protezione e rassicurazione che ci aspettiamo da una struttura medica e dal suo personale. Un ospedale, clinica o studio medico sotto attacco hacker dovrà gestire quindi sia il grande problema del furto di dati sensibili e della loro manomissione, ma anche la questione reputazionale legata alla fiducia dei pazienti: se una struttura viene percepita come “non sicura” i pazienti saranno preoccupati, amareggiati e insoddisfatti.

Far sapere che proteggi i loro dati sensibili con sistemi sempre aggiornati ed efficienti ti aiuterà a instaurare un rapporto di fiducia a 360 gradi con i tuoi pazienti.

CONSIGLIO: Investi in sicurezza cibernetica e informa i tuoi pazienti, che apprezzeranno l’attenzione dedicata alla loro privacy, oltre che alla salute.

Cybersecurity per studi medici e cliniche: come proteggersi

Core Up Srl suggerisce alle aziende operanti nel settore SANITARIO di compiere le seguenti azioni strategiche:

A. **Praticare l'igiene informatica**

Si tratta di un insieme di buone pratiche interne che riducono il rischio legato a virus e attacchi hacker. Molto spesso la fonte di un virus è proprio la chiavetta usb di un dipendente, lo sapevi? Anche le e-mail di phishing vengono inconsapevolmente attivate dal personale interno. Ecco perché occuparsi della formazione interna (cyber awareness) del personale sanitario sui rischi e sulle norme di igiene informatica è il primo passo da compiere (Core Up propone corsi personalizzati).

B. **Scegliere un MSP**

Per la gestione, il monitoraggio e la salute dell'ambiente IT della struttura ricettiva si può incaricare un MSP Managed Service Provider (Provider di servizi gestiti) che da remoto e 24/7 controlla lo stato delle reti e dei sistemi. Un MSP compie tutte quelle azioni necessarie a tenere il più possibile in sicurezza l'infrastruttura IT (rinnovo dell'antivirus, installazione di firewall, manutenzione hardware...) e, in caso di attacco o problemi, interviene tempestivamente per riportare la situazione alla normalità.

C. **Verificare la sicurezza dell'infrastruttura IT**

Per identificare le minacce IT e mitigarne i rischi, è fondamentale partire da una valutazione della sicurezza dell'infrastruttura attraverso due tipologie di verifica: i vulnerability assessment e i penetration test sono metodologie (complementari e consequenziali) che permettono di realizzare un security program su misura, efficace ed efficiente. (Un MSP si occupa anche di questo!)

D. **Studiare una strategia di gestione in caso di incidenti IT**

Pensare a un piano di azione concreto ed efficiente aiuta a mitigare i problemi in caso di incidenti informatici che mandino in tilt i sistemi IT con conseguente perdita dei dati o furto di informazioni sensibili. (Anche in questo caso scegliere un MSP si rivela una scelta vincente!).

Business Provider CORE UP

E se capitasse
al tuo studio medico
o alla tua clinica?

2017, Studio dentistico Dr. Kann, Germania
Lo studio dentistico del Dr. Michael Kann a Wiesbaden subisce un attacco hacker e come risultato tutti i file sul server vengono rinominati e i dati craccati. Gli viene richiesto il pagamento di un riscatto in bitcoin (pari a circa e 4.000,00) entro 48. Superate le 48 ore il riscatto sarebbe raddoppiato. Dopo12 ore ha pagato il riscatto, rientrando in possesso dei dati.

2024, Synlab Italia
A causa di un attacco ransomware i dati personali, i referti, gli esami diagnostici e i documenti d'identità di migliaia di italiani sono stati pubblicati illegalmente sul dark web.

2024, centro analisi-diagnosi Synnovis, Regno Unito
La gang ransomware QiLin ha attaccato Synnovis costringendo alcuni ospedali di Londra a riprogrammare interventi chirurgici e ad annullare centinaia di appuntamenti nei giorni successivi all'attacco hacker.

2018-2023, Mondo
In 5 anni sono stati registrati tra 150-200 attacchi hacker ai dispostivi medici, primi fra tutti i defibrillatori e i pacemaker, per estorcere soldi alle case produttrici e/o mettere in pericolo la salute dei pazienti.

Core Up: il tuo MSP, e non solo...

Scegliere un partner tecnologico MSP come Core Up, che propone il noleggio e la vendita di hardware e software per l'ufficio e servizi di monitoraggio, assistenza e gestione proattiva dell'infrastruttura IT, aumenta i livelli di sicurezza del tuo business, riducendo al minimo i tempi di down-time e i disservizi.
Così potrai ottimizzare tempi e costi, il tutto gestito con comodi canoni periodici personalizzabili.

Cosa possiamo fare per te:

- **SERVIZIO DI MSP (MANAGED SERVICE PROVIDER)**
- **NOLEGGIO DI PC, SERVER, STORAGE, STAMPANTI E MULTIFUNZIONI PER L'UFFICIO/RECEPTION DEL TUO STUDIO/CLINICA**
- **TELEFONIA E CONNETTIVITÀ**

Contattaci per maggiori informazioni: sarà un piacere conoscere la tua realtà e consigliarti i migliori strumenti per far crescere la tua azienda.
T. 030.4194040
M. info@coreup.it / segreteria@coreup.it
W. www.coreup.it