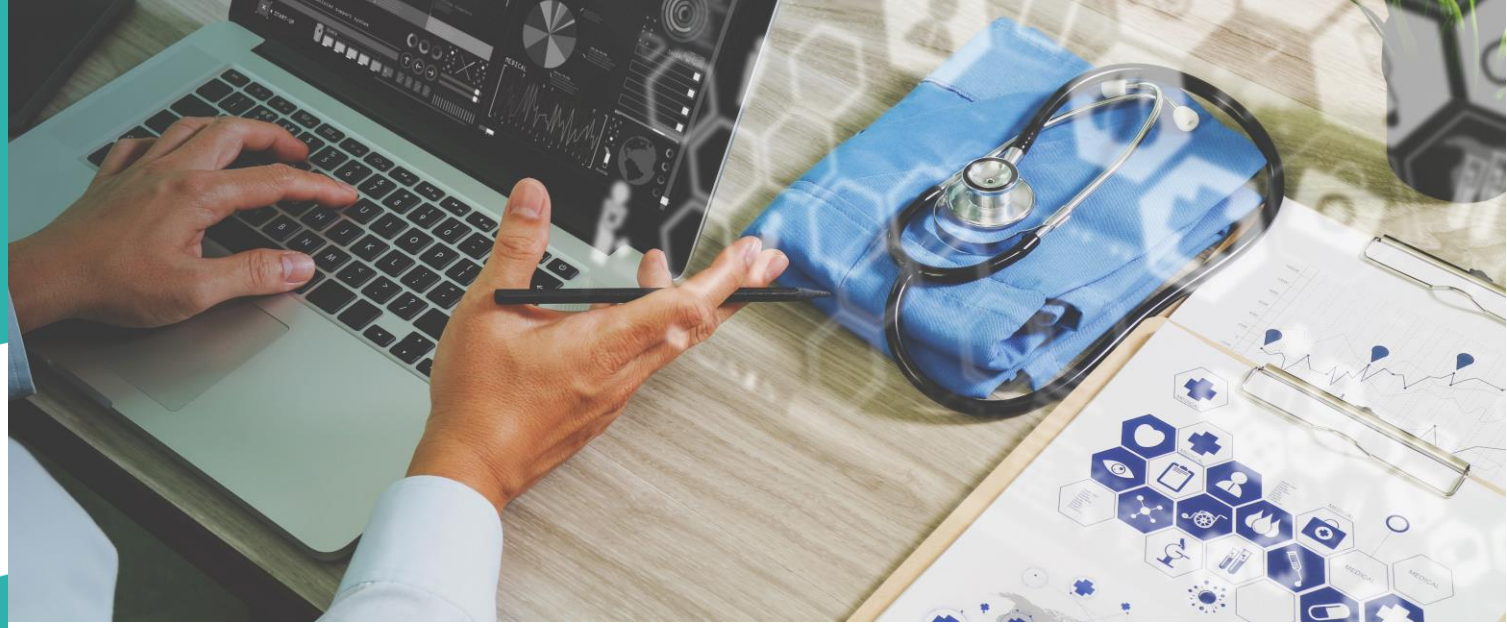
exprivia

future. perfect. simple.

CyberSecurity: la prevenzione ai confini della tecnologia

La Sanità, già minacciata dagli hacker, oggi affronta COVID-19.



L’aumento esponenziale registrato negli attacchi alla Sanità è dettato dalla criticità del servizio e dalla tipologia dei dati gestiti che rendono il settore estremamente appetibile a chi è interessato a trarne profitto illegalmente vendendo i record nel Dark Web o chiedendo denaro in cambio della promessa di ripristinare o non interrompere il servizio stesso.

L’emergenza COVID-19 e il ruolo del Dark Web

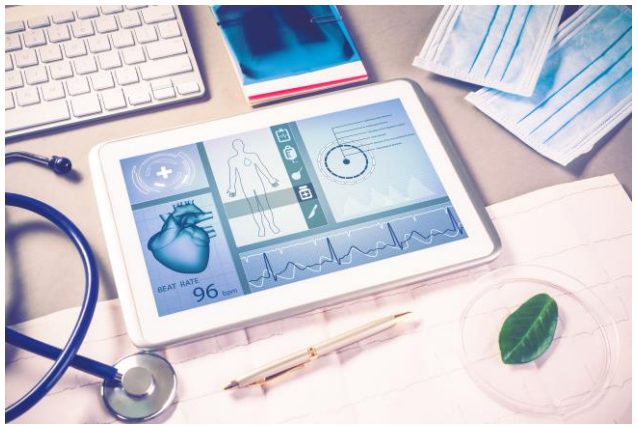
L’emergenza COVID-19 e la necessità di doversi spesso affidare alla Telemedicina per diagnosi remote hanno reso i servizi forniti dalla Sanità ancora più critici.
Se sul Dark Web ieri si potevano trovare record di pazienti, oggi si possono trovare mascherine e medicamenti che suggeriscono come prevenire e curare il coronavirus.

exprivia

future. perfect. simple.

Valutazione del rischio e investimento

Se le minacce rappresentano una evidente criticità, non dissipare il budget dedicato a misure di CyberSecurity con scelte fatte sotto pressione e in emergenza risulta una necessità.
Importante è comprendere l'esposizione alle minacce prima di decidere quale misura adottare.
Exprivia mette a disposizione dei suoi clienti un framework consolidato che studia la tipologia delle minacce e ne valuta il rischio associato in funzione della postura del cliente, dello stato del cliente e di ulteriori misure che sono già state adottate.



Quali sono le misure principali da adottare?

- **Migliorare la capacità di riconoscimento di un attacco:** questo servizio è fornito da un Security Operation Center (SOC) spesso non disponibile presso aziende sanitarie e ospedali. Exprivia offre servizi di monitoraggio espletati dai propri SOC, certificati ISO27001 e specializzati sulla Sanità.

- **Endpoint Detection e Response**: soluzioni in grado di identificare anomalie e bloccare eventuali intrusioni.

- **Microsegmentazione**: necessità di definire delle policies di accesso in funzione di tag assegnati a risorse e persone aventi ruoli e criticità diverse.

- **Unmanaged Endpoint Protection**: non sempre è possibile fornire e gestire direttamente gli apparati in uso agli utenti finali, ma è necessario permettere l'utilizzo di sistemi personali che potrebbero non essere adeguatamente protetti. Tuttavia è possibile identificare e fornire soluzioni tecnologiche che forniscano controlli essenziali senza la necessità di doverli gestire direttamente e senza assumerne il controllo

- **Migliorare la consapevolezza**
  - Bastano corsi di poche ore per ridurre l'incidenza del fattore umano in un incidente di sicurezza.
  - Simulare campagne di malvertisement e phishing in modo da poter identificare le aree di intervento.
  - Simulare tramite cyberrange specializzati sulla Sanità degli incidenti, al fine di verificare come gli attori coinvolti siano in grado di rispondere.