PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4799 di Mercoledì 21 ottobre 2020

Un attacco con ransomware provoca la morte di una persona

Quanto siano temibili gli attacchi con ransomware è ormai noto ai lettori, ma sino ad oggi non si aveva notizia che un tale attacco avesse portato alla morte di una persona.

Nella seconda metà di settembre una università tedesca è stata attaccata con un ransomware. In realtà, i criminali non hanno colpito il computer dell'università, ma il computer della azienda universitaria ospedaliera, cui l'università era collegata. Sono andati progressivamente fuori servizio i 30 server dell'azienda ospedaliera, creando drammatici problemi nella erogazione dei servizi ai pazienti assistiti. In particolare, non è stato possibile attivare le procedure di accoglienza di nuovi pazienti ed una donna, con un grave vizio cardiaco, ha dovuto essere trasferita all'ospedale di Wuppertal, a circa 32 km di distanza. Purtroppo, durante il tragitto la crisi cardiaca si è aggravata e, l'arrivo in ospedale, i medici non sono riusciti a rianimare la paziente. I responsabili informatici dell'università hanno preso contatto con i criminali, informandoli che il loro attacco aveva compromesso i computer dell'ospedale e non dell'università. I criminali allora hanno fornito le parole chiave per il ripristino del sistema. Al momento, le forze di polizia stanno indagando contro ignoti per omicidio.

A fronte di questa drammatica situazione, può essere interessante riferire alcune considerazioni avanzate da uno specialista britannico, che lavora per conto delle compagnie assicurative, che offrono protezione da attacchi informatici. Questo specialista fa parte dello stesso gruppo che offre assistenza per trattare con i rapitori, in caso di richiesta di riscatto. Ricordo ai lettori che mentre negli Stati Uniti ed in Inghilterra è possibile sottoscrivere una polizza assicurativa contro il rischio rapimento, in Italia ciò è proibito. Ecco le interessanti considerazioni tecniche e sociopolitiche, rilasciate da questo specialista.

Con un approccio tutto britannico, questo specialista ha indicato quali possano essere gli elementi che portano a sviluppare un'analisi di costo-beneficio, in fase di gestione di una richiesta di riscatto ransomware.

Ecco gli elementi a favore del pagamento del riscatto:

- con ogni probabilità, il pagamento è la opzione più economica,
- il pagamento può rappresentare una corretta difesa degli interessi dei soggetti coinvolti; si pensi ad esempio ad un paziente ospedaliero che ha bisogno di un immediato soccorso e la cui documentazione sanitaria sia bloccata,
- il pagamento può impedire l'applicazione di sanzioni per la perdita di dati personali e particolari,
- il pagamento permette di non perdere informazioni riservate,
- il pagamento permette di non pubblicizzare la violazione dei dati.

Per contro, è opportuno analizzare anche quali sono i motivi che si oppongono al pagamento di un riscatto:

- il pagamento non garantisce che verrà inviata la chiave di decriptazione corretta,
- il pagamento induce i malviventi a nuove attività criminali, proprio come accadde in Italia quando si verificò un'epidemia di rapimenti di persone,
- il pagamento, che venga pubblicizzato, può danneggiare l'immagine aziendale,
- il pagamento non impedisce certo agli attaccanti di tornare nuovamente l'attacco,
- il pagamento con Bitcoin può esporre l'organizzazione coinvolta rischi economici di varia natura.

D'altro canto, l'esperienza insegna che il contrastare una certa tipologia di attacco informatico fa sì che i malviventi mettano a punto tecniche diverse di attacco.

Insomma, comunque si valuti la situazione, l'attacco per ransomware, portato a termine, rappresenta comunque una situazione di grave crisi per l'azienda coinvolta.

Non è forse meglio mettere a punto una tempestiva e appropriata strategia di archiviazione multipla e protetta dei dati?

Adalberto Biasiotti

---

www.puntosicuro.it