Ransomware: il protagonista del 2021



Gli attacchi di cybersecurity hanno registrato un’impennata eccezionale nel primo semestre 2020 – 850 attacchi – il 7% in più rispetto allo stesso periodo dell’anno precedente.

Sfortunatamente la tendenza in aumento sembra confermata anche per il 2021.

Si prevede, infatti, che i costi globali conseguenti agli attacchi da ransomware raggiungeranno i 20 miliardi di dollari (USD) e che tale tipologia di attacco colpirà un’azienda ogni 11 secondi entro la fine dell’anno. Da sottolineare che il suddetto dato economico non include gli attacchi verso i singoli individui che si verificano più frequentemente rispetto agli attacchi verso le aziende.

Analizziamo di seguito l’impatto devastante dell’attacco ransomware sulle aziende, soffermandoci sulle modalità da adottare per eliminare o ridurre i danni.

Con il termine ransomware si intente un malware che prima rende inaccessibili i dati dei computer infettati e successivamente chiede il pagamento di un riscatto, in inglese ransom, per ripristinarli.

Una volta infettato un pc, il malware si può diffondere all’intera rete aziendale.

Un rapporto del 2017 di Cybersecurity Ventures identificava nel ransomware il tipo di attacco informatico in più rapida crescita. Lo studio prevedeva che i danni per il 2018 avrebbero raggiunto gli 8 miliardi di dollari e gli 11,5 miliardi di dollari nel 2019. Tali previsioni ad oggi sono state confermate dagli esperti del settore.

Da sottolineare che quando si parla di costi riferiti ad attacchi ransomware si fa spesso riferimento solo al pagamento del riscatto; in realtà il costo globale di un attacco di questo tipo è molto più alto e complesso da quantificare.

Nella quantificazione del costo complessivo si devono includere, tra gli altri, i danni derivanti dalla perdita e/o danneggiamento di dati, dall'interruzione del normale svolgimento dell'attività e conseguente perdita di produttività, dal tempo impiegato in indagini forensi, nonché i danni legati alla reputazione aziendale.

Dal momento che si tratta di un'azione criminale relativamente facile da implementare e i rendimenti, come possiamo facilmente dedurre, sono eccezionali, il ransomware si è trasformato nel principale e temuto avversario da fronteggiare per i team di cybersecurity.

Considerato che il principale vettore dell'infezione è l'e-mail e considerato che la gestione della pandemia COVID-19 ha comportato, tra le altre cose, la necessità di implementare il lavoro a distanza possiamo affermare che oggi il rischio è allarmante.

Una volta infettato il sistema, il recupero completo dei dati è spesso impossibile e non vi è garanzia che vengano restituiti anche se il riscatto è stato pagato.

Nella maggior parte dei casi l'azienda paga il riscatto, il cui importo aumenta ogni anno, ma i dati spesso non possono essere recuperati perché distrutti.

Secondo un'indagine Sophos condotta nel 2020 in 26 paesi tra 5000 IT Manager, le aziende che pagano il riscatto spendono fino al doppio in più per ripristinare l'attività aziendale.

A tutto questo si aggiunge il danno di immagine se i dati aziendali sono resi pubblici.

Contromisure efficaci contro il ransomware devono essere adottate in tempi brevissimi da tutte le aziende investendo e lavorando su un duplice approccio: formazione del personale e strumenti tecnici innovativi.

La formazione del personale è fondamentale in quanto, come già rilevato, il vettore dell'infezione da ransomware è solitamente l'e-mail. La formazione continua sottintende un'attenzione sempre alta sul tema e sulle conseguenze, diffondendo strumenti e suggerimenti per identificare le e-mail dannose (attenzione agli allegati o ai link malevoli).

Dal punto di vista tecnico è necessario installare strumenti software di sicurezza volti ad indentificare e mitigare le conseguenze dell'attacco. Importante è anche definire una soluzione in grado di eseguire il backup dei dati in modo sicuro in caso di emergenza.

La difesa informatica deve oltrepassare i confini dei dipartimenti IT in modo che ogni lavoratore capisca esattamente cos'è il ransomware, come infetta le organizzazioni e come si combatte.

Oggi non è possibile eliminare il rischio di attacco ma è doveroso fronteggiarlo e alzare il livello di allerta. In questo senso la formazione del personale rappresenta la più grande speranza per combattere gli attacchi ransomware.

Articolo a cura di **Lisa Da Re**

https://www.ictsecuritymagazine.com/articoli/ransomware-il-protagonista-del-2021/