PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5095 di Venerdì 04 febbraio 2022

In caso di attacco per ransomware chi deve decidere se pagare il riscatto?

Questo tipo di attacco sta diventando ormai talmente frequente, che sono centinaia le aziende che, una volta attaccate, devono rapidamente decidere se pagare o meno il riscatto. Chi deve assumere questa decisione?

Quando un'azienda trova i suoi dati bloccati, a seguito di un attacco per ransomware, deve immediatamente prendere decisioni critiche, che riguardano la stessa sopravvivenza dell'azienda. Sono infatti molte le aziende che, non avendo accesso ai dati e non avendo adottato una politica di backup appropriata, sono prese alla gola e devono assumere in tempi brevissimi decisioni critiche.

A questo punto si pone un quesito critico: chi, nell'azienda, ha la autorità per decidere di pagare un riscatto?

Il consiglio d'amministrazione, oppure l'amministratore delegato, oppure il capo dell'ufficio legale?

È evidente che una decisione di questo tipo è oltremodo critica, soprattutto perché la inaccessibilità ai dati può avere un impatto drammatico sulla operatività dell'azienda, a causa del fermo di alcune attività, una riduzione di produttività, una possibile azione di rivalsa da parte dei soggetti, i cui dati sono stati bloccati dai criminali informatici, e via dicendo.

Come conseguenza, l'azienda può trovarsi nella condizione di dover decidere rapidamente se o meno pagare riscatto, per consentire la ripresa della normale operatività.

Questa decisione talvolta deve essere presa nel giro di poche ore o pochissimi giorni.

A questo punto occorre analizzare, meglio se con l'assistenza dell'ufficio legale, lo statuto dell'azienda, per vedere quali sono i poteri delegati alle varie funzioni di vertice aziendale.

In certi casi la delega di potere è praticamente assoluta, in altri casi vi sono delle limitazioni.

Non dimentichiamo inoltre che in alcuni paesi potrebbe esistere una disposizione legislativa che proibisce il pagamento di un riscatto, come ad esempio avviene in Italia, a fronte del rapimento di una persona.

Chi ha potuto seguire da vicino le vicende legate a rapimenti di importanti personaggi italiani, certamente avrà saputo che il blocco dei conti correnti bancari di tutti i soggetti, potenzialmente coinvolti nel pagamento del riscatto, era una delle prime iniziative, che assumeva la procura della Repubblica che indagava.

È evidente che il problema, circa la decisione su chi deve autorizzare il pagamento del riscatto, diventa meno drammatica, se l'azienda ha attivato tempestivamente un piano per fronteggiare questi eventi di criminalità informatica, e questo piano è stato debitamente approvato dal consiglio d'amministrazione, che a tutti gli effetti rappresenta il vertice decisionale dell'azienda.

Per la verità, alcuni legali hanno eccepito questo ragionamento, ritenendo che la situazione possa assumere un profilo talmente critico, che l'autorizzazione dovrebbe addirittura giungere dalla assemblea degli azionisti, che sono i veri titolari finali del potere aziendale. È evidente che questa impostazione contrasta in maniera stridente con l'esigenza di una decisione rapida, o meglio ancora rapidissima, ed ecco perché può essere esaminata dal punto di vista teorico, ma praticamente è di difficilissima applicazione.

In conclusione, la soluzione migliore è quella di affrontare subito un piano di emergenza, per fronteggiare questo evento criminale e attuarlo nel miglior modo possibile, pianificando subito l'adozione di misura di prevenzione e contrasto e assumendo fin d'ora la decisione critica, di cui abbiamo parlato.

Adalberto Biasiotti

www.puntosicuro.it