Cyber rischi. La simulazione di un attacco ransomware a un'impresa con un fatturato di 120 milioni - Le conseguenze, la reazione e i costi

Scacco all'azienda: così la ripartenza

Dal blocco degli impianti al furto dei dati - Il blackout può durare anche settimane

PAGINA A CURA DI
Enrico Netti

Danni per una ventina di milioni. È questo il costo a cui deve far fronte una media azienda manifatturiera con 120 milioni di ricavi che è vittima di un attacco ransomware o un altro letale virus informatico che blocca completamente ogni attività. Un caso improbabile? Assolutamente no. Nel giugno 2017 il ransomware Petya colpì multinazionali e infrastrutture critiche di tutto il mondo. La scoperta di malware creati per colpire l'Internet delle cose e l'industria 4.0 è continua. Minacce assolutamente da non sottovalutare, come la scorsa settimana hanno ribadito dal World Economic Forum di Davos i potenti del pianeta.

Quanto tempo serve per far ripartire una smart factory messa in ginocchio da un malware? Con quali costi? Quante settimane passano prima di fare ritornare a pieno regime la produzione? Quali le conseguenze per l'impresa? Per dare una risposta a queste domande Il Sole 24 Ore ha simulato il caso di una media impresa con un fatturato di 120 milioni che opera all'interno di una filiera e produce componenti meccanici che, secondo un modello di ordini a programma, vengono forniti ad alcune grandi aziende che li montano nei loro prodotti.

Un giorno sugli schermi dei computer dell'azienda appare la richiesta di riscatto, mentre i dati vengono cifrati. Inizia così lo "shut down" di ogni attività, dall'amministrazione al magazzino.

La top five degli incidenti

Costo medio degli incidenti di sicurezza per grandi aziende nel mondo.
Dati 2017 in milioni di dollari

Fonte: elaborazione Kpmg su dati Kaspersky

«L'accesso alle reti di produzione dall'esterno, passando dalle reti corporate o "di ufficio", nel caso delle Pmi, è una certezza - è la premessa di Raoul Brenna, responsabile della Practice information security&infrastructures di Cefriel, società partecipata da università, imprese e pubbliche amministrazioni che realizza progetti di innovazione digitale e di formazione -. Spesso si registrano "attacchi di filiera", che sfruttano accessi privilegiati concessi a fornitori o clienti per superare il perimetro difensivo esterno. Da qui, il non perfetto isolamento delle reti di produzione permette il transito degli hacker verso macchine a controllo numerico e gli ambienti industry 4.0». L'attacco di ransomware viene denunciato alla Polizia Postale ma per il momento è difficile ipotizzare quando i sistemi verranno ripristinati. Secondo gli esperti in cyber sicurezza consultati dal Sole 24 Ore, il blackout può durare da 7 giorni ad alcune settimane. In un caso, fanno sapere da Cefriel, per eradicare il virus sono serviti addirittura sei mesi.

Si inizia a intervenire per eliminare l'attaccante per poi iniziare a ripristinare le piattaforme e i sistemi della smart factory, dell'internet delle cose e le migliaia di sensori dei macchinari. Situazione analoga anche per i macchinari a controllo numerico (Cnc) senza dimenticare il back office, la parte amministrativa con la contabilità clienti e fornitori per finire con il reparto ricerca e sviluppo. Qui il furto dei dati è molto probabile, perché i pirati sono a caccia di brevetti e progetti. «A maggio con l'entrata in vigore del General data protection regulation le aziende che non hanno comunicato la fuga di dati saranno sanzionate con una multa che può arrivare al 4% del fatturato o a 20 milioni - ricorda Simonetta Candela, partner di Clifford Chance -. In questo contesto è verosimile il diffondersi di polizze assicurative per la gestione del rischio connesso alla cybersecurity».

Per quanto riguarda il personale, le vie per corribili sono diverse, in funzione delle diverse realtà aziendali. Per impiegati o addetti alla produzione, per esempio, si può ricorrere agli ammortizzatori sociali durante lo shut down, oppure si possono fare gli straordinari per ridurre i tempi di riavvio. Lo stesso vale per gli impiegati che devono ricostruire e controllare le posizioni amministrative.

L'azienda avvisa i suoi clienti e fornitori del blocco dell'attività e incarica una società specializzata nella gestione della crisi: un costo da 1.500 euro al giorno.

Clienti e fornitori possono aprire il fronte legale dei contenziosi per inadempimento avanzando richieste di risarcimento per danni. «Nel caso di una transazione è prudente accantonare 30-35mila euro - avverte Marco Torsello, partner di Arblit - mentre se si va in giudizio si può arrivare a 80-150mila». Si arriva così a un conto estremamente salato e forse in parte evitabile se il perimetro di difesa dell'azienda è aggiornato. «Tra gli imprenditori la sensibilità verso la cyber security è molto bassa: oltre la metà si dichiara preoccupata, ma solo il 30% investe nella gestione e nel contrasto» precisa Luca Boselli, partner Kpmg e responsabile per i servizi cyber security.

Nell'industria il tema sta diventando cruciale: domani a Milano si terrà l'Industrial cyber security forum dove si affronterà il tema della difesa delle imprese che hanno intrapreso un percorso di trasformazione digitale.

enrico.netti@ilsole24ore.com

MASCHIO GASPARDO

«Così siamo riusciti a tornare in attività senza pagare riscatto»

Il Gruppo Maschio Gaspardo, produttore di macchine agricole con circa 323 milioni di ricavi previsti nel 2017, 1.800 dipendenti sparsi in 7 stabilimenti produttivi di cui 3 all'estero (Romania, Cina e India) e 12 filiali commerciali nel mondo, è riuscito a debellare, senza pagare alcun riscatto, un attacco criminale di origine sconosciuta sferrato con una mutazione del ransomware Petya.

Per la prima volta la società racconta in tutti i dettagli come si sono svolti i fatti nei giorni del cyber attacco.

La data è quella del 27 giugno 2017, un martedì, quando sugli schermi di tutti i computer dell'azienda è apparsa la richiesta di riscatto con il pagamento di diverse centinaia di euro per "liberare" ogni pc. Immediatamente è stato attivato il piano di disaster recovery previsto dai protocolli aziendali, intervento che ha poi permesso il recupero di tutti i dati aziendali.

Contemporaneamente sono state allertate le autorità di pubblica sicurezza che si sono recate in azienda. Il team interno di 15 tecnici informatici guidati da Massimo Crozzoli con la collaborazione degli specialisti della Polizia Postale ha poi lavorato giorno e notte per far fronte all'emergenza e creare le basi per la ripartenza dei sistemi e degli impianti. Per ragioni dettate dalla prudenza e per salvaguardare la corretta operatività dell'azienda, caratterizzata da un alto livello di automazione, è anche stata precauzionalmente e temporaneamente fermata la produzione degli stabilimenti italiani pur garantendo tutti i servizi primari per i clienti e i fornitori, che non hanno subito disagio. Per rassicurare dipendenti, clienti e fornitori è anche stato diffuso un comunicato stampa in cui si dava evidenza degli avvenimenti.

Progressivamente sono stati testati i sistemi e la produzione negli stabilimenti italiani è ripartita lunedì 3 luglio, con il rientro di tutti i dipendenti negli stabilimenti.