

L'ALLARME DI FILADELFIO EMANUELE, CISO DI CYBERGON

Il food possibile preda degli hacker A rischio magazzino e macchinari

DI ANDREA SETTEFONTI

Paralisi della produzione, contaminazione degli alimenti, esfiltrazione dei dati con richiesta di «riscatto» per sbloccarli o non divulgarli. Sono i rischi che corre il sistema agroalimentare per possibili attacchi, neppure troppo remoti, di pirateria informatica. «Il food vale il 15% del Pil italiano ed è uno dei possibili settori di interesse per un attacco informatico; gli hacker colpiscono dove c'è denaro. Tutte le aziende del settore sono vulnerabili»: lo dice a *ItaliaOggi*, **Filadelfio Emanuele**, chief information security officer & security operation manager presso **CybergON**, la *business unit* di **Elmec Informatica**, dedicata alla sicurezza informatica. Ad essere in pericolo è tutta la filiera, dalla produzione alla distribuzione. «C'è sempre più digitalizzazione nel food per la forte spinta al mercato online; vengono utilizzati strumenti sempre più avanzati, magazzini robotizzati. Questo porta ad un aumento del rischio perché ci sono più accessi».

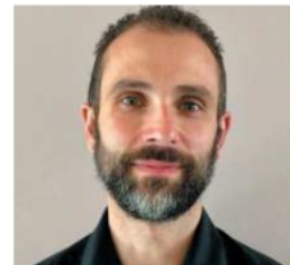
Emanuele svela i rischi possibili: «Uno è il blocco del magazzino; mette in ginocchio un'azienda. Fermo la logistica e chiedo il riscatto. Un'estorsione vera e propria». Del resto, attacchi all'agroalimentare ce ne sono già stati. Ad esempio, quello *ransomware* (per chiedere il riscatto ndr) a **JBS**, produttrice brasiliana di carne bovina che possiede più di 150 stabilimenti negli Usa e in tutto il mondo. «Una dimostrazione di forza da parte del gruppo criminale **REvil**, conosciuto anche come **Sodinokibi**, che ha interrotto un quinto della fornitura di carne. Il pagamento di un riscatto di circa 11 mln di dollari in *Bitcoin*, è stato condannato duramente dal Congresso americano e dall'**FBI**», ricorda Emanuele. Ma c'è di

più: «I macchinari sono sempre più automatizzati; si possono compiere azioni di modifica dei parametri di produzione per immettere sul mercato un prodotto modificato rispetto al dovuto o deteriorato. Si crea un danno d'immagine importante che va oltre il valore economico», spiega il Ciso di CybergON.

Anche in Italia si è avuto un attacco: «Un'azienda di salumi si è ritrovata sotto attacco *ransomware* con tutti i dati crittografati. Questo ha bloccato la produzione». Emanuele tiene a fare una raccomandazione. «Quando una azienda scopre di essere sotto attacco, è importante sapere da dove sono entrati e cosa hanno fatto. Quindi, contrariamente all'agire comune, la prima cosa da non fare è spegnere tutto, perché questo impedisce di capire da dove sia arrivato l'attacco e cosa ha fatto».

La tecnologia informatizzata trova applicazione in tutta la filiera. Ci sono bracci robotizzati dotati di una tecnologia che permette di avere un ritorno maggiore sulla qualità finale del prodotto; la sensoristica IoT consente controlli qualità sempre più stringenti nel mondo del food. Nello stoccaggio delle materie prime e dei prodotti finiti l'innovazione aumenta la capacità di gestione delle scorte e l'efficienza del trasporto.

— © Riproduzione riservata — ■



Filadelfio Emanuele

ARTICOLO NON CEDIBILE AD ALTRI AD USO ESCLUSIVO DEL CLIENTE CHE LO RICEVE - 3041



Superficie 37 %