Attacco ransomware a Luxottica e ospedali, le vulnerabilità note da anni

Blockchain, AI&Cybersecurity *è la rubrica curata da* ***Alessandro Civati****, Ceo* ***Lirax****: notizie, spunti ed aggiornamenti (tecnici) sul nuovo mondo digitale che sta cambiando le nostre vite. Per consultare tutti gli articoli clicca qui*.

In pochi giorni due attacchi ransomware avrebbero sfruttato la stessa vulnerabilità nota da alcuni mesi. Colpite la società Luxottica e un ospedale tedesco. A questo secondo attacco sarebbe anche collegata una vittima.

Attacco ransomware a Luxottica, i dettagli

Il 21 settembre alcuni media nazionali ed internazionali hanno riportato la notizia di un attacco hacker alla società Luxottica, che ha riguardato in particolare le sedi Agordo e Sedico, in provincia di Belluno, provocando il blocco della produzione e la sospensione dei turni degli operai.

Se in un primo momento si è parlato di gravi problemi informatici, con la rete fuori uso, il blocco dei computer e l'impossibilità ad eseguire qualsiasi operazione, sarebbe poi stato confermato un attacco ransomware, un tentativo di violare i sistemi informatici che non avrebbe avuto esito positivo grazie ai meccanismi di difesa attivati dalla società. Solo per precauzione sarebbero stati disconnessi momentaneamente i server.

Nessun data breach, ma danno alla produzione e all’immagine

Nessun data breach dunque, ma rimane un grave danno sia alla produzione che all’immagine della società a conferma delle sempre maggiori minacce informatiche che gravano sulle aziende.

Secondo quanto riportato dal sito *Bleeping Computer* i criminali informatici avrebbero sfruttato una vulnerabilità nota dall’inizio dell’anno nei prodotti VPN di Citrix for Cyber-Attacks, con la quale ottenere credenziali per l’accesso e la diffusione all’interno di una rete. La stessa vulnerabilità che avrebbe consentito l’attacco ransomware ad un ospedale tedesco pochi giorni prima, dalle conseguenze ben peggiori.

Una vulnerabilità provoca conseguenze tragiche in Germania

In questo caso infatti, l’attacco, che ha portato all’interruzione dei sistemi e alla sospensione delle attività ambulatoriali e di emergenza, sarebbe strettamente correlato al decesso di una persona che non ha potuto ricevere le cure sanitarie urgenti di cui necessitava, ritardate a causa del trasferimento in altra struttura. Se le indagini della polizia tedesca dovessero confermare questa correlazione, si tratterebbe della prima vittima di un attacco cyber.

Secondo quanto emerso e riportato da diversi siti web di settore, l’attacco sarebbe stato indirizzato per errore all’ospedale. Il vero obiettivo era un’università, e gli hacker avrebbero fornito la chiave per decrittare i server non appena informati dell’errore. Ma tanto è bastato ad impedire di garantire le cure necessarie e a mettere in luce, se ancora ce ne fosse bisogno, la necessità di un impegno maggiore sul

fronte della cyber security.

Il lavoro nell’ambito del contrasto alle minacce informatiche, nonostante la crescente consapevolezza, sembra ancora molto. Secondo un rapporto di *Check Point*, infatti, l’80% degli attacchi ransomware di questi primi mesi del 2020 sfruttava vulnerabilità note, alcune addirittura da sette anni. Purtroppo questi avvertimenti vengono ancora troppo spesso ignorati o quantomeno sottovalutati.

L’autore: Ing. ***Alberto Perin****i, esperto di Cyber Security dal 2006 impiegato nella ricerca e sviluppo di sistemi di difesa informatica.Ha lavorato presso diverse realtà in Svizzera, Uk, Italia ed Israele come cyber security manager gestendo progetti di SOC/CSIRT (Security Operational Center), cooperando anche con università Italiane nella ricerca di nuovi sistemi dedicati all’IOT – OT.*

> *Attacco ransomware a Luxottica e ospedali, le vulnerabilità note da anni*