Quotidiano
12-04-2025
Pagina 3
Foglio 1

Treviso
IL GAZZETTINO

Diffusione: 7.658

Asolo Dolce, i pirati: «Pagate il riscatto»

▶Attaccati i sistemi dell'azienda: informazioni rubate e mail cancellate. Poi la richiesta di soldi per limitare i danni

▶Cento imprenditori a palazzo Giacomelli per la cybersicurezza «Raid lievitati del 15%, pmi trevigiane indietro sulla formazione»

L'ALLARME

ASOLO L'azienda Asolo Dolce è finita sotto attacco hacker. La celebre azienda dolciaria, che produce un fatturato di 40 milioni di euro e che conta un'ottantina di dipendenti, è finita tra le vittime dei pirati informatici che terrorizzano tutto il comparto industriale trevigiano. Gli hacker sono riusciti a violare i sistemi dell'azienda. E da qui hanno rubato una lunga serie di dati. Dopodiché si sono rivolti alla stessa azienda con minacce e con la richiesta di pagare un riscatto per poter avere indietro le informazioni sensibili. In caso contrario, hanno detto, i dati in questione verrebbero resi disponibili a tutti nel dark web. La ditta è stata vittima di un attacco particolarmente aggressivo. C'è stata in primis la sottrazione dei dati. Ma non solo. «Gli hacker hanno pure cancellato tutte le caselle di posta elettronica» spiegano dall'azienda. Il modus operandi dei pirati informatici è sostanzialmente sempre lo stesso: prima l'acquisizione dei dati privati relativi a persone, clienti o fornitori; poi il caricamento di un pacchetto degli stessi dati nel mercato nero online e di seguito il ricatto economico all'azienda colpita. Se non si paga, è la minaccia, il materiale viene o pubblicato online, senza filtri, oppure venduto al miglior offerente. Un'azione criminale che tiene conto soprattutto della lunga serie di complicazioni (anche sotto forma di costi) che le aziende si trovano ad affrontare in questi casi, considerando gli obblighi a cui sono legate nei confronti del garante della privacy e dei propri dipendenti. Dal punto di vista degli organi di controllo spesso non è sufficiente essere coperti da una protezione standard per certificare il proprio impegno nel tutelare i dati: ci si espone così a ulteriori eventuali sanzioni. Per questo motivo, a prescindere dalla presenza o meno di una copertura assicurativa, gli hacker continuano a considerare probabile la scelta dell'azienda di pagare l'importo per risolvere in fretta e contenere i costi.

IL QUADRO

Gli attacchi hacker contro le aziende ormai rappresentano una vera e propria emergenza. Solo negli ultimi due anni sono aumentati del 15%, come evidenzia l'ultimo rapporto Clusit. E le Marca non è un'isola felice. Giusto per citare gli ultimi casi, tra le società finite nel mirino figurano Mom, azienda degli autobus e delle corriere, Adrenalina di Caerano, specializzata in abbigliamento sportivo, Fantin Group di Istrana, produttrice di infissi. E così via. Fermo restando che le variabili in gioco sono diverse, ogni attacco costa in media 60mila euro al giorno alle società che finiscono nel mirino.

Ieri un centinaio di imprenditori si sono ritrovati nella sede di Confindustria Veneto Est a palazzo Giacomelli per il corso organizzato da Unis&F proprio sulla cybersicurezza nelle piccole e medie imprese: «Sono le più esposte agli attacchi informatici». Le più colpite sono in particolare quelle del manifatturiero. E il sistema produttivo al momento si ritrova a rincorrere. La conferma arriva dal sondaggio su 45 aziende del trevigiano eseguito da Sitora Salaewa, ricercatrice dell'Università di Padova.

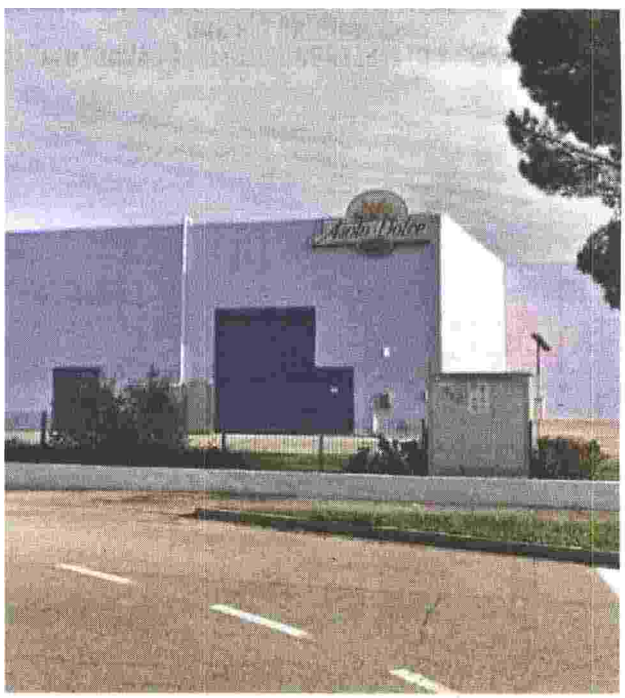
GLI ATTACCHI ARRIVANO CON LE MAIL TRUFFA E ATTRAVERSO L'INSTALLAZIONE DI SOFTWARE DANNOSI

LA RICERCA, PIU' DELLA META' DELLE AZIENDE NON HA ANCORA UNA PROCEDURA PER DIFENDERSI

NELLA MARCA

Da una parte il 98% delle imprese si è dotato di una figura responsabile della sicurezza informatica. Parallelamente, però, solo il 33% del personale riceve una formazione regolare sulla gestione dei dispositivi fisici che controllano le operazioni e i processi industriali. «Tra questi, sono molti quelli che credono di non aver subito attacchi - avverte Salaewa - la mancanza di formazione rischia di dare una falsa percezione». A questo si aggiunge il fatto che tre quarti delle imprese trevigiane non eseguono analisi di sicurezza e non aggiornano regolarmente i loro sistemi di operational technology. Anche il semplice wifi, impiegato dal 73%, se non usato al meglio rischia di rappresentare una porta d'ingresso per i pirati informatici: «Va protetto meglio». Più delle metà delle imprese, inoltre, non ha ancora codificato una procedura per rispondere agli attacchi arrivati dall'esterno. Quelli più comuni nella Marca arrivano attraverso il phishing, le mail truffa inviate a raffica per rubare dati, il ransomware (software dannoso che crittografa i dati o blocca l'accesso a un dispositivo in cambio del pagamento di un riscatto) e i classici malware.

L.V. - M.F.



NUOVO ALLARME Dopo la società Mom anche Asolo Dolce