Pirati informatici in azione lo scorso ottobre

Attacco hacker all'Azienda ospedaliera Un «sms» a chi ha subito il furto dei dati

• Sono 658mila i file finiti nel «dark web» Aoui sta avvisando le vittime e mette a loro disposizione lo psicologo

CAMILLA FERRO

Pirati informatici Monitor spenti negli uffici dell'Aoui dopo l'attacco degli hacker

L'Azienda Ospedaliera Universitaria Integrata di Verona ha iniziato a mandare ieri un sms ad alcuni dei pazienti rimasti vittima dell'attacco hacker subito la sera dello scorso 22 ottobre. Li informa che alcuni loro dati personali di natura sanitaria e amministrativa sono finiti in mano ai criminali della rete.

I pirati del web rubarono infatti una serie di informazioni (non quelle custodite nel Sio, il Sistema Informatico Ospedaliero entrato in funzione nel giugno 2023 in cui sono archiviate cartelle cliniche elettroniche, dossier sanitario e fascicolo sanità km zero) e chiesero un cospicuo riscatto per rilasciarle.

Non avendolo Aoui pagato, i ladri hanno diffuso i dati in loro possesso nel Dark Web cioè nella «rete oscura» (è quella parte di Internet dove sono presenti siti nascosti, accessibili solo con un determinato browser e utilizzando connessioni speciali).

Si tratta per la precisione di 658.828 file contenenti informazioni parziali e incomplete di utenti e collaboratori dell'Azienda ospedaliera, sia di natura sanitaria che amministrativa, file che una task force composta da 65 gruppi di professionisti (sanitari, informatici, amministrativi e giuristi) hanno ricostruito attraverso un certosino lavoro di analisi durato mesi: l'obiettivo di tanta fatica era appunto quello di analizzare la tipologia delle notizie violate per informarne poi i diretti interessati, a seconda del livello di rischio. È stata stilata infatti una classificazione delle informazioni esfiltrate, da quelle «rosse» (foto di pazienti, lettera di dimissione, referto di visite ed esami, diagnosi oncologica e studi clinici) ossia dalle più importanti oggetto appunto di sms a quelle via via meno per le quali non è previsto nessun invio di messaggio ai pazienti: le «arancioni» (foto non riconoscibile ma riconducibile, referto esami, anamnesi e consegne di reparto con nomi), le «gialle» (foto non riconoscibili, prescrizione, ricetta, richiesta esami, certificazioni, raggi, anagrafica, consensi informati), le «blu» (dato amministrativo, modulistica, dati sanitari non riconducibili, documenti personali, verbali riunioni).

Cos'è successo
Il 22 ottobre 2023 un attacco informatico ha violato dati sensibili di utenti e dipendenti Aoui poi pubblicati nel dark web

«Oltre alle procedure attivate appena abbiamo subito l'attacco, imposte dalla legge», spiegano dalla direzione a Borgo Trento, «come ad esempio l'informativa al garante della privacy, la notifica all'Agenzia Cyber sicurezza nazionale e la denuncia alla Polizia postale, abbiamo poi provveduto in questi mesi ad informare l'utenza secondo il Piano Strategico di Comunicazione rivolto agli interessati, sia a livello interno con newsletter indirizzate ai dipendenti che all'esterno con lettere, Faq, spazi appositi acquistati sui giornali, canali social e il portale aziendale».

«Quanto agli sms personalizzati inviati agli utenti rientranti nella classificazione rossa», continuano dalla direzione generale, «li invitiamo a leggere sul sito aziendale le Faq cioè le "domande frequenti" che mirano a chiarire l'accaduto e a fornire, in modo pratico, informazioni precise». Inoltre, chi tra i pazienti «rossi» ne sentisse la necessità, Aoui mette a disposizione anche il supporto psicologico. Per loro ma anche per tutti gli altri è comunque possibile inviare una mail per richiedere informazioni a comunicazioni.databreach@aovr.veneto.it allegando copia di un documento di identità.