L'Aquila, hackerata l'Asl «Presi i dati dei pazienti»

▶In tilt il sistema sanitario provinciale: nei reparti saltano visite e prenotazioni

▶Trafugati oltre 500 giga di informazioni, tra cui anche i conti bancari dei dipendenti

IL CASO

L'AQUILA L'attacco è scattato nel cuore della notte, per opera dei cyber criminali del cosiddetto "gruppo Monti", una galassia variegata dietro cui si celano gli hacker che utilizzano il "ransomware", un programma informatico malevolo in grado di intrufolarsi nei dispositivi danneggiando o sottraendone i dati, per poi chiedere un riscatto - spesso in valute digitali - in cambio della loro restituzione. Nell'elenco dei blitz del "ransomware Monti" si è aggiunta l'Azienda sanitaria locale dell'Aquila che è ora alle prese con una crisi senza precedenti, «una catastrofe» come sussurra un medico che chiede l'anonimato. L'incursione ha infatti mandato in tilt il sistema informatico di ospedali e distretti sanitari di tutta la provincia, con gravissime ripercussioni sull'attività medica e sull'assistenza.

CARTA E PENNA

In quasi tutti i reparti, Pronto Soccorso in primis, si è tornati a carta e penna per la registrazione dei pazienti, ma in alcuni casi sono state bloccate visite e prenotazioni. Non solo. Mentre l'azienda, nella sua unica, assai scarna comunicazione, ha parlato di «dati sensibili al sicuro», i pirati del Web, nella loro "rivendicazione", sostengono il contrario, ovvero di avere tra le mani molte informazioni, tra cui quelle sui pazienti affetti da Hiv. Il gruppo criminale dice anche di aver trovato nell'infrastruttura informatica dell'Asl 1 Abruzzo una «situazione di vulnerabilità sfruttabile», tale da permettere una massiccia sottrazione di dati. Con la minaccia della loro diffusione pubblica, online, se non dovesse essere pagato il riscatto. In tutto sarebbe stato trafugato materiale per 522 gigabyte.

La rivendicazione è apparsa, come avviene sempre in casi simili, sul "Data leak site (Dls)" di Monti, ovvero una sorta di sito internet ufficiale della "gang", ed è stata riportata dai principali blog di sicurezza e crimini informatici.

PERSONALE COSTRETTO A CATALOGARE TUTTO CON CARTA E PENNA L'ATTACCO È STATO RIVENDICATO DAL "GRUPPO MONTI"

L'Asl è stata letteralmente travolta dalla crisi, ma non ha confermato, al momento, la portata della gravità. Da ieri sono al lavoro squadre di cyber esperti arrivate anche da fuori città, ma i tempi di ripristino delle reti sono avvolti nel mistero. Ci sono previsioni ottimistiche di alcuni giorni, ma secondo alcuni, lavorando a pieno regime con una quindicina di persone, potrebbero volerci addirittura due o tre settimane. I danni sono in ogni caso ingentissimi e le conseguenze rischiano di trascinarsi per un tempo molto lungo.

Per questa mattina il manager, Ferdinando Romano, ha convocato la prima riunione della task force costituita anche su input della Regione che ieri ha inviato all'Aquila il dirigente del servizio Sanità Digitale, Camillo Odio, per una prima ricognizione. L'assessore alla Salute, Nicoletta Verì, segue l'evolversi in prima linea. Il summit di stamattina servirà anche per fornire le prime informazioni ufficiali al personale che sta operando in condizioni di obiettiva difficoltà.

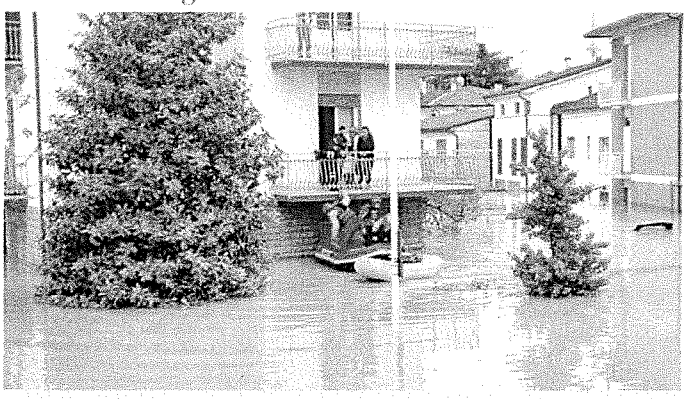
GLI SFORZI

Va detto che il personale, con uno sforzo considerevole, sta cercando di portare avanti l'attività, pur con ritardi e difficoltà. Le conseguenze più pesanti si registrano per richieste di esami e prenotazioni. Il Cup, il Centro unico di prenotazione, è sostanzialmente bloccato, anche se si sta tentando di garantire le prestazioni per chi aveva già fissato gli appuntamenti e le urgenze per chi ne avesse bisogno, con la collaborazione dei reparti. Resta il grande interrogativo sul recupero dei dati relativi alle liste di attesa. Sono state invece sospese tutte quelle attività che necessitano della consultazione di database o di processi informatici. È il caso, ad esempio, delle visite dermatologiche, anche oncologiche e del controllo dei melanomi. Gli esami del sangue vengono garantiti per urgenze ed emergenze, ma i referti vengono stampati su carta. Stessa cosa viene fatta per i tamponi Covid. Si procede anche ai ricoveri, anche in questo caso attraverso la comunicazione tra reparti. Insomma, negli ospedali sembra di essere tornati indietro di quindici o vent'anni, quando tutto o quasi veniva registrato o annotato su registri cartacei. Il possibile furto dei dati - che l'Asl non ha né confermato né smentito, probabilmente in attesa delle verifiche più puntuali in corso - ha messo in grande allarme non solo i pazienti, ma anche i dipendenti, che temono la violazione di informazioni anche di carattere economico (conti bancari in primis). Una volta risolta l'emergenza bisognerà capire quali e quante siano state le falle della Rete informatica dell'Asl aquilana che, secondo alcuni esperti, potrebbe essere stata violata attraverso le classiche email "phishing", quelle che inducono alla comunicazione truffaldina dei dati.

Stefano Dascoli

STAMATTINA SUMMIT PER FARE IL PUNTO PER IL RITORNO ALLA NORMALITÀ POTREBBERO VOLERCI DUE O TRE SETTIMANE

La decisione Il governo stanzia 10 milioni di euro



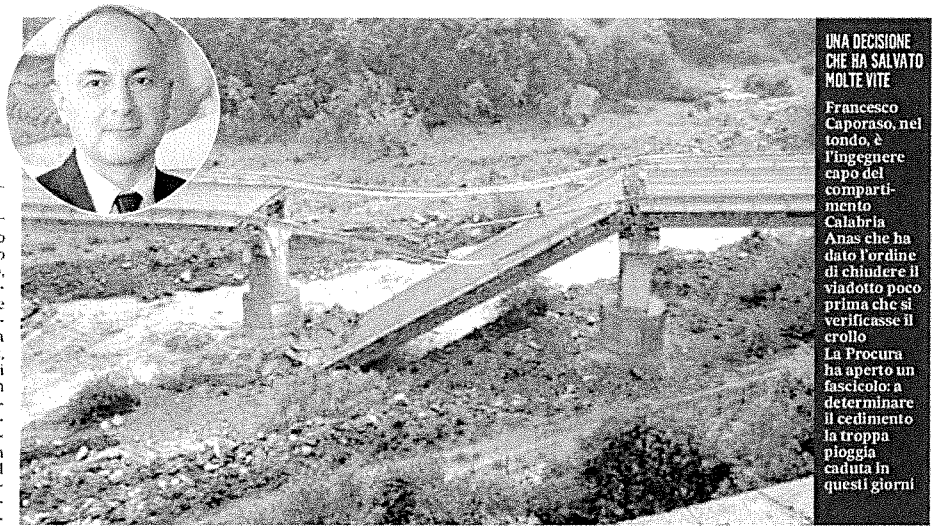
Stato di emergenza per l'alluvione in Romagna

In Romagna si contano i danni dopo l'ondata di maltempo che ha causato allagamenti, frane e due morti. Il governo ieri ha deciso, su proposta del ministro Nello Musumeci, lo stato di emergenza nazionale per le alluvioni. Stanziati 10 milioni di euro. Oltre alle province romagnole di Ravenna e Forlì-Cesena, hanno riportato danni anche le aree emiliane di Reggio, Modena, Bologna e Ferrara. Nel Ravennate, soprattutto a Faenza, Castel Bolognese e Faenza ci sono ancora centinaia di sfollati. Ha commentato il governatore dell'Emilia-Romagna, Stefano Bonaccini: «Grazie a Meloni e Musumeci per lo stato di emergenza in tempi rapidissimi»

Lavori utili

Giustizia, intesa tra Telefono Rosa e ministero sui minorenni

Sono sei, ma le richieste sono molte, i detenuti che parteciperanno al protocollo nazionale siglato tra il Ministero della Giustizia e il Telefono Rosa per i lavori di pubblica utilità. I dati sono stati forniti ieri dall'onorevole Simonetta Matone e dal Telefono Rosa. Il progetto si pone infatti alcuni obiettivi: una Campagna guida sicura per sensibilizzare i ragazzi che troppo spesso si mettono alla guida ubriachi o sotto l'effetto di stupefacenti, diventando un pericolo per loro stessi e gli altri. Non solo. Gli ambiti sono diversi. I partecipanti avranno anche la possibilità di capire cosa significa subire violenza all'interno delle mura domestiche. «Il protocollo è al livello Nazionale, siamo la prima Associazione che si occupa di violenza di genere a portare avanti questo percorso. Sono coinvolti non solo tutti i Telefoni Rosa d'Italia, ma anche le Associazione e le Fondazioni con le quali abbiamo una collaborazione già attiva. Vogliamo portare questo progetto in tutte le province d'Italia», ha detto la presidente del Telefono Rosa, Maria Gabriella Carnieri Moscatelli.



UNA DECISIONE CHE HA SALVATO MOLTE VITE

Francesco Caporaso, nel tondo, è l'ingegnere capo del compartimento Calabria Anas che ha dato l'ordine di chiudere il viadotto poco prima che si verificasse il crollo La Procura ha aperto un fascicolo: a determinare il cedimento la troppa pioggia caduta in questi giorni

«Troppa acqua, ho chiuso il viadotto» Così il dirigente eroe ha evitato la strage

LA STORIA

LONGOBUCCO (COSENZA) Sono più o meno le 18 di mercoledì quando nel territorio di Longobucco, nella zona della Sila Greca cosentina, la pioggia incessante e la piena del fiume Trionto causano il cedimento della campata centrale del viadotto Ortiano 2, lungo la Strada Statale 177 Dir di Longobucco dal km 6.500, in provincia di Cosenza. Per fortuna non ci sono né vittime, né feriti e tutto grazie al monitoraggio costante dei tecnici Anas in condizioni di allerta meteo. Il tratto di strada, infatti, era chiuso al traffico dopo l'ordine lungimirante dell'ingegnere Francesco Caporaso, capo compartimento Calabria: una decisione che ha evitato conseguenze tragiche. «In occasione dell'allerta meteo, le strutture Anas presidiano le tratte stradali interessate dagli eventi segnalati soprattutto nel caso in questione, dove il regime torrentizio del corso d'acqua, il Trionto, richiede un'attenzione particolare - ha spiegato l'ingegnere - Questa attività ha consentito di seguire l'evoluzione dei fenomeni indotti dal torrente sull'infrastruttura in più punti, e di adottare tutte le precauzioni necessarie, fino alla chiusura totale del tratto di strada».

IL SILA-MARE È CROLLATO INTORNO ALLE 18, MA UN'ORA PRIMA UN INGEGNERE DELL'ANAS AVEVA GIÀ FERMATO LE AUTO

LE AUTORITÀ

A Caporaso e ai vertici Anas sono arrivati i complimenti del presidente della Regione Calabria, Roberto Occhiuto. «Non fosse stato per loro, a quest'ora probabilmente si starebbe parlando di una tragedia con vittime. Invece questa volta, la competenza e la prontezza hanno evitato una tragedia».

Poche ore prima del crollo, infatti, era stato diramato l'ordine di chiusura al traffico in entrambe le direzioni e a tutti i mezzi, dopo che le squadre Anas avevano evidentemente notato che qualcosa non andava. E quel qualcosa che non andava era un pilone del viadotto immerso nel fiume Trionto che piano piano ha cominciato ad avere problemi, mentre uno dei giunti cominciava ad allargarsi.

Il video amatoriale del crollo ha fatto il giro dei social e in pochi minuti è diventato virale. «Immagini incredibili - racconta il governatore -. Si tratta di un ponte costruito soltanto nove anni fa dai Comuni del posto, i Comuni della Comunità montana Destra Crati - Sila Greca, che crolla in questo modo. Sono immagini che ricordano il crollo del ponte Morandi, che ha mietuto tantissime vittime. Vittime che non ci sono state per la prontezza dell'Anas».

L'INCHIESTA

La Procura della Repubblica del Tribunale di Castrovillari, competente territorialmente, ha aperto un fascicolo al fine di risalire alle responsabilità del crollo. Il viadotto era stato costruito nel 2014 così come parte della strada, la cui progettazione risale agli anni '70. La magistratura ha posto sotto sequestro l'intera arteria e quindi per gli abitanti della Valle del Trionto diventa problematico raggiungere le zone di mare. Le altre arterie della zona, infatti, presentano gravi problemi di percorribilità. L'Amministrazione comunale di Longobucco ha disposto una unità di crisi presso il Municipio, dove si segue l'evolversi della situazione. Tutte le scuole di ogni ordine e grado sono rimaste chiuse.

Il viadotto era stato aperto al traffico nel 2016 dalla Regione Calabria e l'Anas ne aveva acquisito la gestione nel 2019. I particolari delle cause del crollo sono in corso di accertamento da parte dei tecnici di Anas.

Bruno Palermo

L'Aquila

OROLOGIO "CARDILLI", OGGI L'INAUGURAZIONE

Sarà inaugurato oggi alle 11 lo storico orologio "Cardilli", posto sulla vetrina di quella che fu la prestigiosa gioielleria Cardilli sotto i portici a due passi da piazza Duomo. Grazie al Rotary, infatti, l'orologio è stato sottoposto a un'operazione di restauro che restituisce dopo il sisma un pezzo della memoria storica cittadina.

Fax: 0862 410164
e-mail: aquila@ilmessaggero.it

Venerdì 5 Maggio 2023
www.ilmessaggero.it

IL CASO

Asl sotto attacco hacker ospedale paralizzato odissea per visite e referti

▶Stamattina riunione della task force convocata dal manager Romano

▶Difficoltà per richieste e prenotazioni Fedele: «Pubblicata sul Web un'ecografia»

Per capire cosa sta succedendo all'ospedale dell'Aquila, da mercoledì notte sotto un gravissimo attacco hacker che ha paralizzato l'intero sistema informatico dell'Asl, basta mettere il naso in Pronto soccorso. Dove sembra di essere tornati indietro di decenni: si arriva e si viene registrati con carta e penna. Una situazione, quella del "San Salvatore", che più di un camice bianco, rigorosamente senza il crisma dell'ufficialità (c'è un regolamento interno molto ferreo sulla comunicazione), definisce «catastrofica» anche se va chiarito che l'attività medica viene comunque portata avanti, seppur con rallentamenti e oggettive, pesanti, difficoltà. L'ombra più pesante è quella del furto dei dati sensibili. A questo proposito nella tarda serata di ieri il consigliere regionale del M5s, Giorgio Fedele, ha rivelato che o cyber criminali autori dell'hackeraggio avrebbero pubblicato sul "Deep Web" (la porzione di Internet che non viene indicizzata dai motori di ricerca) il referto di una ecografia ginecologica di una paziente. «A questo punto - dice Fedele - l'interruzione dei servizi sarebbe solo la punta dell'iceberg di un problema ben maggiore. Va fatta luce». Per stamattina il manager, Ferdinando Romano, ha convocato una riunione, una sorta di task force aziendale, così come auspicato anche dalla Regione che, per mezzo dell'assessore alla Salute, Nicoletta Veri, ha chiesto una verifica. A questo proposito ieri in ospedale si è recato il dirigente regionale del servizio Sanità Digitale.

Si diceva dei disservizi, che sono concentrati essenzialmente in due grandi ambiti, le richieste di prestazioni e le prenotazioni. Blocco totale al Centro unico prenotazioni (Cup): non è possibile effettuare la prenotazione di prestazioni agli sportelli, né tramite call center o servizio online. Chi ha una prenotazione può, però, presentarsi allo sportello Cup per il pagamento e la registrazione del ticket nel giorno fissato per la prestazione con foglio di prenotazione ed impegnativa. Chi invece deve prenotare una prestazione urgente deve invece andare sportello Cup che contatterà il reparto interessato. Stop anche alle visite dermatologiche prenotate in Dermatologia Generale ed Oncologica per l'ambulatorio melanoma. Difficoltà anche per gli esami istologici, laddove i referti non siano stati stampati.

A sinistra i pazienti all'interno del Pronto soccorso e in basso il manager Ferdinando Romano che ha convocato oggi un vertice della task force

COMUNICAZIONE

L'Asl per ora ha scelto di comunicare pochissimo. Bocche cucite e informazioni con il contagocce. Nulla si sa sugli eventuali tempi di ripristino né sulla reale portata dell'attacco. «Quanto accaduto - ha detto ieri l'europarlamentare - è una situazione che va monitorata con attenzione. I dati sanitari e la sicurezza nella gestione degli stessi rappresentano una problematica che sta assumendo un peso sempre più rilevante anche all'interno dell'Unione Europea. Sto lavorando come relatore ombra per il Gruppo Identità e Democrazia nella Commissione Envi del Parlamento Europeo sul dossier legato allo "Spazio europeo dei dati sanitari", ponendo l'attenzione sulla necessità di semplificare la burocrazia proteggendo allo stesso tempo i dati».

Stefano Dascoli

L'intervista Walter Tiberti

«Potrebbero volerci settimane, servono buone pratiche»

Il professor Walter Tiberti è docente di sicurezza informatica dell'Ateneo dell'Aquila. A lui "Il Messaggero" ha chiesto di delineare il perimetro di cosa è accaduto all'Asl.

Professore, che cosa è un attacco hacker e come si concretizza?

«Si tratta di un attacco lanciato da criminali informatici che può avvenire tecnicamente in diversi modi. Ultimamente si tende ad attaccare le persone dietro ai sistemi con e-mail di phishing (email truffa per carpire dati personali, ndr) per poi allargare l'attacco. L'azione si può anche portare avanti, ad esempio, rubando l'identità di un dipendente di un'azienda».

Che tipo di organizzazione è Ransomware Monti?

«In realtà i gruppi sono molti e cambiano nome spesso per ovvie ragioni. Prendono di mira target selezionati e provano poi ad attaccare ad ampio spettro per poi rivendicare la loro azione. Serve soprattutto per farsi un nome nel loro campo. In questo caso, Ransomware Monti è un tipo di attacco abbastanza conosciuto, dietro ci sono poi diverse persone che lo usano per "infettare"».

È plausibile la richiesta di riscatto?

«Sì, è plausibile e si fa, lo dice del resto la parola stessa "Ransom" che vuol dire riscatto, ma il fatto che si paghi, come avviene nel caso di un rapimento, non vuole dire avere la certezza di riavere le informazioni eventualmente trafugate».

«GRUPPO CONOSCIUTO CHE PRENDE DI MIRA TARGET SELEZIONATI LA PORTATA DELL'AZIONE È DA QUANTIFICARE»

È possibile dunque che abbiano rubato dati sensibili?

«Sì, ovviamente è possibile, ma bisogna dire che va atteso il risultato dell'analisi forense che sicuramente si sta facendo per capire esattamente cosa è stato portato via».

Quanto tempo richiede l'analisi e soprattutto quando si può pensare ad un ripristino del sistema?

«Non si può dire, non si può dare una tempistica così. Normalmente dipende dalla configurazione della rete e dei sistemi. A volte può essere un fatto di un'ora, altre volte potrebbero volerci giorni o settimane. Questo a seconda della vastità dell'attacco, se sono stati colpiti più apparati, quindi è tutto da verificare».

Cosa deve fare ora la Asl I per recuperare i dati?

«Per il recupero dei dati è necessario che siano state portate avanti innanzitutto delle buone pratiche preventive come il backup o la procedura di *incident response*. Queste cose permettono all'infrastruttura di essere meno vulnerabile e di limitare i danni e i dati rubati. Non è sempre così, ma avere più backup assicura che in caso di un attacco di media entità si riesca a tornare attivi a breve».

È possibile risalire ai responsabili, alle persone fisiche?

«È molto difficile perché spesso sono di fuori Europa e non si rintracciano, usano sempre pseudonimi. In generale anche se si fa una denuncia la strada è molto difficile, a volte si può arrivare ad un risultato ma la pratica è sempre molto lunga».

Daniela Rosone

L'EUROPARLAMENTARE DE BLASIS «PROBLEMA SERIO LAVORO AL DOSSIER PER PROTEGGERE I DATI DEGLI UTENTI»

SANITÀ » COMPUTER IN TILT

Ospedali, altro giorno di passione Gruppo hacker rivendica l'attacco

Continuano i disagi nelle strutture. La Asl presenta una denuncia e la Polizia postale sta indagando I sedicenti pirati informatici dicono di essersi impossessati dei dati, anche di pazienti sieropositivi

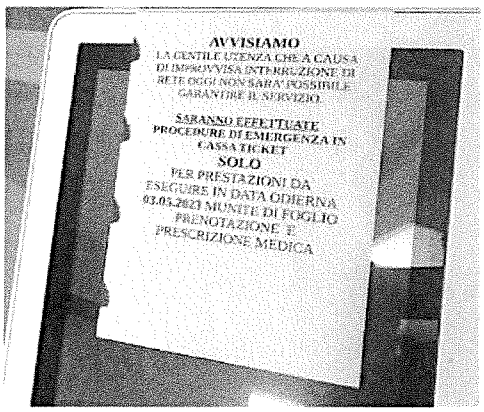
di Monica Pelliccione

L'AQUILA

Il responsabile dell'attacco sferrato al sistema informatico della Asl Avezzano-Sulmona-L'Aquila ha un nome. Si tratta del gruppo Monti ransomware che ieri, sul data leak site (Dls), ha pubblicato un annuncio in cui rivendica l'azione. Un post che riporta chiaramente «l'avvenuta compromissione informatica della Asl 1, con 522 Gb (gigabyte) di dati esfiltrati dalla infrastrutture It dell'azienda sanitaria». In altre parole, gli hackers del gruppo Monti avrebbero estrapolato dati sensibili dei pazienti. Rivendicazione che, sulla scorta di quanto accaduto in altri episodi simili, potrebbe portare alla richiesta di un riscatto per evitare la diffusione e l'utilizzo improprio delle informazioni. La Asl ha immediatamente sporto denuncia: da due giorni, i tecnici di una società di Roma specializzata in attacchi hacker stanno lavorando nella sala operativa dell'azienda, fianco a fianco con la Polizia postale: va avanti la silenziosa battaglia per verificare se e quali dati siano realmente in possesso dei cybercriminali. Ieri, intanto, negli ospedali, nei distretti e negli ambulatori si è vissuta un'altra giornata di passione, tra disagi per gli operatori, code e disservizi per gli utenti.

VERIFICHE IN CORSO

Il sistema informatico della Asl è stato paralizzato, provocando rinvii e difficoltà nei servizi operativi e nelle prenotazioni negli ospedali (L'Aquila, Avezzano, Castel di Sangro, Pescina e Tagliacozzo), nei distretti sanitari e negli ambulatori. Rallentamenti nella gestione che hanno colpito, in particolare, le prenotazioni al Cup, ma anche esami o visite specialistiche. «Abbiamo sporto denuncia alla Polizia postale che è intervenuta immediatamente e sta lavorando da due giorni insieme ad esperti di una task force di cybersecurity, che non si sono fermati neppure la notte», afferma il direttore amministrativo della Asl, **Stefano Di Rocco**, «non possiamo ancora sapere se siano stati prelevati dati: siamo nella fase iniziale delle verifiche, ma stiamo operando con il massimo della celerità per risolvere il problema nel più breve tempo possibile». Mercoledì scorso la Asl aveva diffuso una nota evidenziando come «nessun dato sanitario o sensibile è stato trafugato o perduto. L'archivio informatico è integro». Ma dopo la rivendicazione dell'attacco, il timore è che informazioni private siano finite nella mani sbagliate.



L'avviso negli uffici del Cup dell'ospedale San Salvatore (foto Raniero Pizzi)

Utenti chiedono informazioni all'ospedale di Avezzano (foto Antonio Oddi)

LA RIVENDICAZIONE

La conferma arriva da un post comparso ieri mattina sul data leak site di Monti ransomware, uno dei gruppi hackers più attivi e temibili a livello internazionale, che riporta «l'avvenuta compromissione della Asl 1 Avezzano-Sulmona-L'Aquila». Si parla di «dati esfiltrati dalle infrastrutture It dell'azienda sanitaria». Nella rivendicazione degli hackers viene specificato che «molteplici vulnerabilità hanno consentito il download di dati sui pazienti sieropositivi». Se quanto riportato nel messaggio fosse vero, si tratta di dati ultra sensibili, che possono essere pubblicati dalla cybergang e che lasciano supporre che gli hackers dispongano di informazioni del software di archiviazione e di dati provenienti dal laboratorio di sequenziamento del Dna. Su questi aspetti si concentra l'attività investigativa della Polizia postale e del team di esperti in cybercecurity.

DATI SENSIBILI

Il timore è che possa essere stato violato l'archivio digitale, copiando informazioni riferite ai pazienti, con la minaccia di una successiva diffusione. Fino alla serata di ieri all'azienda sanitaria non era ancora arrivata una richiesta di riscatto, che potrebbe essere inoltrata nelle prossime ore: almeno, questo è il *modus operandi* del gruppo Monti ransomware a detta degli esperti. E a farlo supporre è soprattutto il messaggio di rivendicazione dei cybercriminali che hanno utilizzato specifici codici e softwarer per penetrare i server dell'azienda sanitaria.

» NESSUN RISCATTO CHIESTO FINORA

Una speciale squadra di esperti arrivata da Roma lavora a risolvere il caso

«Aggiornare i sistemi operativi»

Parla Teti, professore di cyberintelligence: ecco che cosa può essere accaduto

Il professore Antonio Teti

L'AQUILA

«Il messaggio diffuso dal gruppo Monti ransomware di hackers, che rivendica l'attacco alla Asl Avezzano-Sumona-L'Aquila, parla chiaro: dice che hanno esfiltrato dalle infrastrutture informatiche dell'azienda circa 522 gigabit. Significa che hanno prelevato svariati dati sui pazienti. Se questa rivendicazione fosse vera, sarebbe molto grave in quanto si tratta di dati non solo personali, ma sensibili». A parlare è **Antonio Teti**, responsabile settori informativi e innovazione tecnologica dell'Università D'Annunzio e professore di cyberintelligence. Uno dei massimi esperti in Italia in materia. Teti spiega che «il Ransomwar è un'applicazione che penetra un sistema informatico, preleva i dati e li cancella o li cifra. Sulla base di questa operazione criminale, gli hacker possono chiedere un riscatto per non diffondere i dati, se rubati, o renderli di nuovo leggibili se criptati. Può essere accaduto questo, secondo la rivendicazione del gruppo Monti, che potrebbe aver prelevato e copiato parte del database della Asl».

Le verifiche in corso scioglieranno ogni dubbio. «Solitamente, ad un annuncio di questo tipo fa seguito la richiesta di un riscatto», afferma il professor Teti, che chiarisce: «Per gli attacchi hacker vengono utilizzati dei codici in grado di penetrare i server sfruttando delle vulnerabilità che possono derivare da una versione non aggiornata o obsoleta dei sistemi operativi utilizzati, da un file non funzionante o da altri elementi. A questo punto è facile estrarre i dati».

Ma come prevenire che ciò accada?

«È consigliabile aggiornare sempre i sistemi operativi delle piattaforme server e fare corsi di formazione al personale sulla cultura della sicurezza informatica», dice Teti, «due precauzioni che consentono di ridurre il rischio di attacchi o di danneggiamento dei sistemi informatici. Soprattutto la Pubblica amministrazione deve farlo, avendo in mano i dati sensibili di tante persone. Nel caso della Asl, informazioni sullo stato di salute, codici fiscali, sesso. Mettere le mani sul database dei diabetici o dei malati oncologici, significa possedere una base di informazioni che ha un valore enorme nella commercializzazione di prodotti farmaceutici specifici». *(m.p.)*

GUERRA INFORMATICA » CONTROMISURE ALL'AQUILA

Dati sensibili rubati dagli hacker: ora l'Asl chiama il super esperto

L'avvocato Celotto incaricato di gestire le conseguenze della violazione della privacy dei pazienti
Ha avuto ruoli di primo piano al fianco di 6 ministri tra cui Barca, inviato speciale per la ricostruzione

di Luca Tomassoni

L'AQUILA

Un problema di grande entità richiede figure di grande rilievo per essere gestito e risolto. Lo hanno ben compreso all'Asl di Avezzano, Sulmona e L'Aquila, che ha deciso di chiamare il super esperto in ambito legale **Alfonso Celotto** per fronteggiare le conseguenze del violentissimo attacco hacker, che ha provocato il furto e la diffusione online dei dati sensibili di pazienti e dipendenti. Si parla di milioni di documenti riservati, tra cui referti medici, per un totale di 522 Gigabyte di materiale finito alla mercé di tutti – anche malviventi informatici – sul blog nel dark web del gruppo di cybercriminali di origine russa "Ransomware Monti".

Sulla violazione dei dati sensibili si è espresso duramente il Garante della privacy, mentre indagano, per conto della Procura dell'Aquila, anche polizia postale e Agenzia per la cybersicurezza nazionale, oltre ai tecnici chiamati dall'azienda stessa. La violazione della privacy non è un problema solo per le vittime, che rischiano di subire, tra le altre cose, truffe e ricatti online, ma anche per l'azienda, che potrebbe dover fronteggiare azioni legali. Questo mentre, a un mese e mezzo dall'attacco, l'Asl sembra ormai praticamente tornata alla normalità.

L'INCARICO

«Privacy. Conferimento incarico»: è questo l'oggetto della deliberazione del direttore generale dell'Asl **Ferdinando Romano,** datata 16 giugno, con cui viene incaricato Celotto per attività «in seno al gruppo di lavoro costituito in forma straordinaria» e a «compenso per l'attività da espletare al valore minimo» previsto dalla normativa.

Nel motivare la decisione di incaricare Celotto, nella delibera si premette, «che la notte tra il 2 e il 3 maggio 2023 l'Asl 1 Abruzzo Avezzano, Sulmona, L'Aquila ha subito un attacco informatico di tipo ransomware». E ancora, nelle motivazioni si spiega che «in ragione della rilevanza e assoluta novità dell'evento, la direzione strategica aziendale ritiene necessaria, anche sotto il profilo legale, una specifica assistenza coordinata sia in relazione ai rapporti con le amministrazioni centrali e locali, sia con il Garante per la protezione dei dati personali, sia in ordine a eventuali contenziosi relativi all'evento in argomento». Quindi si ritiene necessario «affidare incarico a professionista individuato per la specifica esperienza e competenza in materia».

IL SUPER ESPERTO

Alfonso Celotto del resto è una figura di rilievo nazionale. È avvocato e docente universitario di Diritto costituzionale e Diritto pubblico comparato. È anche scrittore e opinionista. Ma è stato soprattutto capo di gabinetto e capo Ufficio legislativo dei ministri Bonino, Calderoli, Tremonti, Trigilia, Guidi e Barca. Con quest'ultimo ha operato all'Aquila, visto che il ministro **Fabrizio Barca** tra il 2011 e il 2013 è stato inviato speciale del governo Monti per la ricostruzione.

L'INGIUNZIONE DEL GARANTE

Celotto sarà quindi chiamato a gestire, almeno dal punto di vista legale, le conseguenze della grande violazione dei dati sensibili di pazienti e dipendenti dell'Asl. La sua nomina arriva a pochi giorni dalla scadenza del tempo limite dato all'Azienda sanitaria per comunicare la violazione ai singoli utenti interessati, come ingiunto dal Garante della privacy. Per l'Autorità, che ha dato solo 15 giorni all'Azienda sanitaria, non basta la comunicazione generica effettuata dall'azienda tramite avviso pubblico.

Il direttore generale dell'Asl 1 Ferdinando Romano e l'avvocato Alfonso Celotto, incaricato dall'azienda

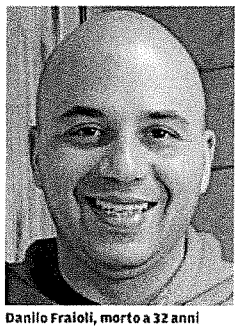
L'ALTRO AFFANNO

Gran Sasso Acqua, ancora disagi negli uffici

Di sicuro anche oggi gli sportelli al pubblico della Gran Sasso Acqua resteranno a funzionalità limitata. Per i prossimi giorni, invece, si attendono nuove comunicazioni da parte della società acquedottistica. Gli esperti incaricati dalla Gsa sono infatti ancora alle prese con l'opera di bonifica di tutti i sistemi informatici aziendali dopo l'attacco hacker. I cybercriminali sono ancora ignoti: non ci sarebbero né richieste di riscatto né rivendicazioni, anche perché il loro attacco sembra essere stato sventato in tempo, dato che gli archivi della Gsa erano e sono custoditi nel server di una ditta esterna. Sotto attacco sono invece finiti i computer aziendali della Gran Sasso Acqua, destinatari di pec infette. In particolare un computer, da cui il file che si sospetta essere un virus è stato aperto. Nei giorni scorsi il presidente della Gsa Alessandro Piccinini ha rassicurato sulla sicurezza dei dati sensibili e sull'entità limitata dei danni informatici, scusandosi con gli utenti aquilani per i disagi dovuti alla necessità di spegnere i sistemi per verifiche e bonifica.

Precipita dal ponte di Pietrasecca

Avezzano in lutto per un 32enne. Allarme lanciato all'alba da un passante sull'A24



Danilo Fraioli, morto a 32 anni

di Pietro Guida

CARSOLI

Un volo dal punto più alto del viadotto di Pietrasecca, già scenario in passato di numerosi drammatici episodi. A lanciarsi nel vuoto è stato **Danilo Fraioli**, un giovane di Avezzano che aveva 32 anni. Ha fermato la sua auto e ha superato le barriere di protezione lasciandosi cadere. La tragedia è avvenuta dopo le 4.30 di ieri, poco prima del sorgere del sole, lungo l'autostrada A24, in direzione Roma. Sulle cause del gesto estremo non ci sono spiegazioni. Il giovane non ha lasciato alcun messaggio ai genitori o agli amici.

Secondo la ricostruzione dell'accaduto, il 32enne è sceso dalla sua auto, una Fiat Panda, fermandola a bordo della carreggiata, sulla corsia di emergenza. Ha lasciato la portiera aperta e si è arrampicato sulla rete di protezione alta oltre un metro, realizzata alcuni anni fa proprio con l'obiettivo di scoraggiare questi episodi.

In passato il ponte di Pietrasecca, a pochi chilometri dall'uscita di Carsoli, veniva chiamato "viadotto della morte" poiché scenario di numerosi suicidi. Tra cui quello del 1995 che coinvolse un'intera famiglia romana – madre e tre figli adulti – probabilmente vittima di usura.

La macchina ferma di Danilo Fraioli, senza nessuno a bordo, è stata notata da un viaggiatore che ha lanciato l'allarme. Sul posto – la zona è nel territorio comunale di Carsoli – è arrivata una pattuglia della polizia autostradale dell'Aquila. È stato poi richiesto l'intervento dei vigili del fuoco e di un'ambulanza del 118. Ma purtroppo per il giovane avezzanese non c'era più nulla da fare.

Gli inquirenti stanno cercando ulteriori elementi per poter capire i motivi che abbiano portato il ragazzo a compiere il gesto disperato. La salma è stata messa a disposizione dell'autorità giudiziaria, così come la macchina, recuperata dal servizio stradale. Distrutti dal dolore i genitori del giovane. Una vita difficile quella di Danilo, costellata di difficoltà che però aveva cercato di superare con l'aiuto della famiglia. Da diverso tempo era anche volontario della Croce Blu Marsica soccorso di Avezzano. Gli amici lo descrivono come «un componente indispensabile». Dai volontari viene ricordato come «un giovane socievole, disponibile in associazione, molto attento e sensibile nell'aiuto di persone disabili».

I funerali si terranno domani alle 10 nella chiesa di San Giovanni ad Avezzano.

L'Aquila

■ L'Aquila - Viale Corrado IV, 50
■ Centralino Tel. 0862/61444-5-6
■ Fax Tel. 0862/22483
■ Pubblicità Tel. 0862/319301
■ e-mail: red.aquila@ilcentro.it

Al vostro fianco, da sempre.
PACINI
0862 24 593
www.onoranzefunebripacini.it

SANITÀ » CAOS E DISAGI IN TUTTA LA PROVINCIA

Asl sotto attacco hacker, sistemi in tilt

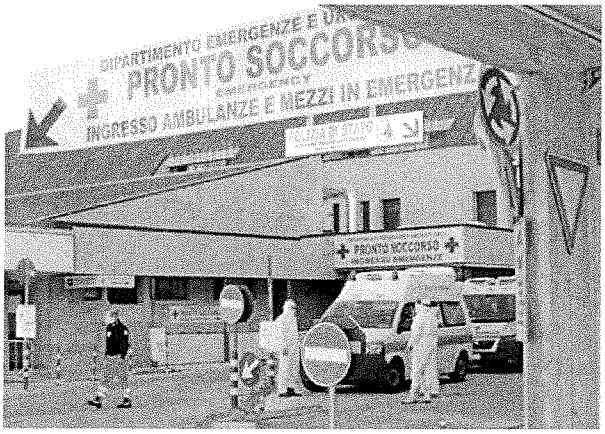
Blocco informatico per prenotazioni, esami e Pronto soccorso. L'azienda: «Esperti esterni al lavoro, dati sensibili al sicuro»

di Luca Tomassoni

L'AQUILA

Un sistema sanitario provinciale totalmente nel caos, tornato improvvisamente all'epoca del cartaceo per il blocco di tutto il suo apparato l'informatico. Dall'ospedale dell'Aquila a quelli di Avezzano, Sulmona, Castel di Sangro, Pescina e Tagliacozzo, passando per i distretti sanitari e gli ambulatori: i disagi sono enormi e diffusi, tra code, rinvii e disservizi, che colpiscono soprattutto prenotazioni al Cup, esami, visite e gestione del Pronto soccorso, ma anche gli interventi chirurgici programmati. La confusione va avanti da 24 ore: ieri sera la situazione era tutt'altro che risolta.

Questa mattina si terrà un altro vertice della Asl, che sarà una sorta di consiglio di guerra, perché dalle 4 della notte di ieri l'azienda sanitaria combatte una silenziosa battaglia informatica con l'aiuto di esperti esterni della cybersicurezza. La Asl si sta infatti difendendo da un gruppo di hacker che l'ha messa sotto assedio. Tesoro da difendere è innanzitutto il suo archivio digitale, che al momento sarebbe al sicuro ma che, se violato e clonato dai cybercriminali, potrebbe portare a una minaccia di diffusione dei dati sensibili degli utenti. Ma si cerca ovviamente anche di riattivare i sistemi informatici interni dell'azienda sanitaria totalmente bloccati. Il rischio è che arrivi una richiesta di riscatto per sbloccare la situazione.



A sinistra il Pronto soccorso dell'ospedale dell'Aquila, dove sono stati tanti i disagi per l'attacco hacker Qui accanto il direttore amministrativo della Asl Stefano Di Rocco

LA BATTAGLIA INFORMATICA

«Sono in corso tutte le attività di verifica tecnica per ripristinare nel minor tempo possibile la piena operatività dei sistemi informatici in totale sicurezza», ha scritto la direzione della Asl Avezzano-Sulmona-L'Aquila in una nota diffusa nel pomeriggio, ammettendo un «blocco del sistema informatico che si è registrato a seguito di un attacco hacker». E ancora: «I nostri tecnici e gli esperti di una task force di cybersecurity si sono messi immediatamente al lavoro e stanno portando avanti un'analisi tecnica sui server aziendali, definendo l'area da cui sono partiti i "malware" (sorta di virus informatici, *ndr*) che hanno colpito i server. Si spera di poter risolvere il problema al più presto ma possiamo rassicurare che nessun dato sanitario o sensibile è stato trafugato o perduto. L'archivio informatico è integro».

La rassicurazione è importante, anche perché nelle prime ore dopo l'inizio della battaglia informatica si parlava di dati criptati dagli hacker. Un altro punto fermo lo ha aggiunto il direttore amministrativo della Asl **Stefano Di Rocco**, al di fuori della nota dell'azienda: «Al momento non abbiamo ricevuto alcuna richiesta di riscatto».

«AL MOMENTO NESSUNA RICHIESTA DI RISCATTO»

Di Rocco smentisce che stia accadendo come in altri casi recenti. Ma la battaglia digitale coi criminali è ancora in corso

IL PERICOLO E GLI ALTRI CASI

Al di là degli enormi disagi, è proprio questo il pericolo, che i cybercriminali ricattino la Asl per non diffondere pubblicamente i dati sensibili o per sbloccare il sistema. Del resto è quanto sta accadendo in altre azioni informatiche che stanno colpendo grandi enti italiani in questi giorni. È il caso dell'attacco "ransomware" – come viene definito dal punto di vista tecnico – della gang "Lockbit" ai danni del gruppo sanitario Multimedica, a cui fanno capo l'ospedale San Giuseppe di Milano e l'Ircss Multimedica di Sesto San Giovanni. Ma anche di quello che gli hacker di "Medusa Locker" stanno compiendo contro la società acquedottistica campana Alto Calore. In entrambi i casi, dopo giorni di battaglia, i due gruppi di cybercriminali hanno rivendicato gli attacchi, diffuso pubblicamente una parte di dati sensibili degli utenti e chiesto un riscatto oneroso. Azioni criminali di questo tipo vanno avanti da tempo in tutto il mondo, ora tocca alla Asl aquilana difendersi.

Insegnante muore con il kit del suicidio

La 63enne originaria dell'Aquila ma residente in Trentino: in Italia altri 8 acquirenti online di veleno

L'indagine è dell'Interpol

L'AQUILA

Una insegnante originaria dell'Aquila, 63 anni, è morta dopo aver utilizzato un kit per aspiranti suicidi. **A.D.L.** è la protagonista di questa spaventosa storia nata due anni fa in Canada, dilagata nel Regno Unito e ora è arrivata in Italia. Una storia raccontata dal *Corriere della Sera*. L'Interpol si è fatta consegnare le foto scattate dai carabinieri di Borgo Valsugana (Trento) in casa della vittima, trovata senza vita lo scorso 4 aprile nel suo appartamento, distesa sul letto. Accanto, aveva un biglietto per i familiari: «Mi dispiace. Sono troppo malata, troppo dolore, non avevo altra scelta, addio». E poi una lettera con la spiegazione di come aveva fatto per togliersi la vita. Così, la Direzione centrale della polizia criminale, approfondendo le indagini, ha scoperto che il nome della donna era nella lista clienti di un uomo dell'Ontario di nome **Kenneth Law**, ex ingegnere aerospaziale e poi chef a Toronto, che per due anni ha gestito alcuni siti web (ora chiusi) vendendo «veleno» per aspiranti suicidi: mascherine facciali e nitrito di sodio. In Italia i suoi kit risultano acquistati da nove persone (l'insegnante originaria dell'Aquila è morta ad aprile era tra questi); le altre otto sono state rintracciate in collaborazione con questure e carabinieri nelle province di Roma, Milano, Napoli, Monza, Lecco, Caserta, Bologna, Trento e Pavia. La Procura di Trento ha aperto un'inchiesta per istigazione al suicidio. Si tratta di un prodotto apparentemente innocuo, il nitrito di sodio, utilizzato nell'industria alimentare come colorante. Tuttavia alcuni grammi, diluiti nell'acqua, insapore e incolore, sono letali. Il Times di Londra ha riferito le parole di Kenneth Law intercettato fuori da una farmacia di Mississauga, Ontario. L'uomo ha raccontato di essere entrato nel business dopo aver visto sua madre soffrire a seguito di un ictus, vantandosi di aver spedito i suoi prodotti in tutto il mondo, anche a «centinaia di clienti» in Gran Bretagna. La storia esplose due anni fa.

«Non sto facendo niente di male» si è difeso così dalle contestazioni del suo interlocutore «sto solo vendendo un prodotto. Non sto assistendo il suicidio di nessuno. È la vostra scelta». *(c.s.)*

L'Aquila

PAGANICA, TROVATO MORTO IL 59ENNE ZUPPELLA

Commozione a Paganica e in città per l'improvvisa scomparsa, a soli 59 anni, di Marco Zuppella. Molto conosciuto e stimato in città e nella comunità di Paganica, Zuppella è morto a causa di un malore improvviso, nella sua abitazione, un alloggio dei Map di Paganica 2. La morte risalirebbe ad alcuni giorni fa.

Fax: 0862 410164
e-mail: aquila@ilmessaggero.it

Sabato 6 Maggio 2023
www.ilmessaggero.it

IL CASO

Attacco hacker all'Asl un mese per il ripristino

▶I tempi per riattivare la Rete sono lunghi
Vertice con i medici: piano per l'emergenza

▶Preoccupa la sottrazione di dati sensibili
La Postale indaga, ma c'è il nodo sicurezza

Potrebbe volerci anche un mese per ripristinare il sistema informatico dell'Asl violato da un pesante attacco hacker che ha mandato in tilt le procedure e permesso ai criminali del Web, a differenza di quanto sostenuto dall'azienda, di trafugare dati sensibili per oltre 500 gigabyte tra referti, analisi, cartelle cliniche, esami. Uno di questi, come ha rivelato il consigliere regionale Giorgio Fedele (che ieri ha chiesto nuovamente di fare luce sulla vicenda) è stato pubblicato sul "Deep Web", la porzione di Internet "sommersa" e non indicizzata dai motori di ricerca: un chiaro segnale degli intenti del gruppo criminale che si cela dietro la galassia del "Ransomware Monti", già conosciutissimo per attacchi del genere che hanno lo scopo di chiedere un riscatto in cambio della restituzione delle informazioni. La Polizia postale indaga contro ignoti per accesso abusivo, danneggiamento e interruzione di pubblico servizio. Difficilissimo risalire alle persone fisiche che hanno condotto l'operazione, nascoste dietro pseudonimi e spesso residenti fuori Europa. Ieri la direzione aziendale ha convocato, di buon mattino, i capi dipartimento per mettere a punto un piano di carattere funzionale che nelle intenzioni dovrebbe consentire di portare avanti l'attività ospedaliera limitando i disagi. Si tratta di una serie di indicazioni che sostanzialmente prevedono il ricorso alla registrazione cartacea di prestazioni e prenotazioni, ma è chiaro che alcuni settori, come il laboratorio analisi e tutta la Diagnostica, avranno maggiori difficoltà. E ci sono anche attività del tutto bloccate: è il caso dei controlli dermatologi (anche l'ambulatorio melanoma) e delle prenotazioni di prestazioni a sportelli Cup, call center e servizio online.

Ospedale ancora in tilt per l'attacco degli hacker

RIPERCUSSIONI

Al di là dell'aspetto medico e dell'assistenza, a preoccupare sono tutte le ripercussioni legate alla fuga di dati, che apre scenari inquietanti per i pazienti e per i dipendenti. I risvolti della violazione della privacy sono molteplici e potrebbero comprendere anche eventuali richieste di risarcimento danni per la mancata tutela. In ogni caso squadre di esperti in cyber sicurezza sono al lavoro intanto per quantificare il danno e poi per procedere ai backup e alla "bonifica" del sistema prima di un ripristino che si annuncia lungo e complesso. L'azienda continua a tenere una discutibilissima linea di non-comunicazione, preferendo non informare la collettività di ciò che sta accadendo e si sta facendo. Un dato è granitico: il servizio informatico Asl presenta certamente delle carenze numeriche (9 dipendenti in provincia, di cui 3 all'Aquila e responsabile vacante da tempo, a Teramo, tanto per citare un esempio, si parla di numeri doppi) e anche tecniche legate alla sicurezza, come evidenziato già da diverso tempo da alcune relazioni interne che evidenziano la necessità di valutare la sicurezza e l'integrità della Rete.

Stefano Dascoli

Air Show di Preturo

Morte di un pilota, niente Frecce Tricolori ma la due giorni si terrà regolarmente

In considerazione del grave lutto che ha colpito le Frecce Tricolori, con la tragica scomparsa del capitano Alessio Ghersi, tutti gli appuntamenti di Maggio del Gruppo Acrobatico sono stati posti in riprogrammazione. Tra questi c'è anche quello previsto nell'ambito dell'Air show all'aeroporto dei Parchi di Preturo il 27 e 28 maggio prossimi. «La speranza è che l'esibizione delle Frecce Tricolori possa comunque essere confermata con la certezza, in caso negativo, della ricalendarizzazione nei prossimi mesi, per rendere omaggio alla memoria del pilota e onorare al meglio i 100 anni dell'Aeronautica militare» hanno detto l'assessore Paola Giuliani con delega all'Aeroporto e il consigliere comunale, con delega alla valorizzazione dello scalo, Livio Vittorini. L'iniziativa prevista all'aeroporto in ogni caso si svolgerà regolarmente con la partecipazione dell'Aeronautica Militare: nei prossimi giorni sarà reso noto il programma con esibizioni per più di 5 ore di spettacolo con velivoli storici, interventi acrobatici con velivoli singoli, pattuglie con velivoli convenzionali e jet, nonché la possibilità per gli utenti di effettuare un giro in mongolfiera.

L'Aquila

"L'AQUILA INCONTRA" ALLA NECROPOLI DI FOSSA

Appuntamento alla Necropoli di Fossa per l'evento di questa settimana con "L'Aquila Incontra". Stamane alle ore 10, accompagnati da Alberta Martellone della Soprintendenza archeologica, belle arti e paesaggio per le province dell'Aquila e Teramo, si visiterà il sito che si trova nei pressi della Stazione di Fossa e del Villaggio Map.

Fax: 0862 410164
e-mail: aquila@ilmessaggero.it

Domenica 7 Maggio 2023
www.ilmessaggero.it

IL CASO

Attacco hacker alla Asl scattano due inchieste

▶In campo l'Agenzia per la Cybersicurezza nazionale e l'ufficio centrale della Polpost

▶Palumbo (Pd) chiede al sindaco Biondi di riferire subito in Consiglio comunale

Sull'attacco hacker alla Asl dell'Aquila, in campo l'Agenzia per la Cybersicurezza nazionale e l'ufficio centrale della Polizia postale. Per gli esperti quella in atto in questo momento, è una sorta di gioco di scacchi: prima si riesce a capire come il "virus" ha lavorato e prima è possibile capire dove c'è stata la falla. Gli esperti non escludono un possibile intervento anche dello stesso Garante per la Privacy per valutare quali sistemi di protezione dati sono in possesso alla Asl e quale è stata la risposta della stessa per evitare il furto di 500 gigabyte, tra referti, analisi, cartelle cliniche, esami ma anche richieste di vaccinazioni. Informazioni ora nelle mani di criminali del web, che a quanto pare hanno approfittato delle ore notturne (anche se sul punto sono ancora in corso gli accertamenti) per "succhiare" le migliaia di file per ottenere un riscatto per evitarne la stessa pubblicazione, magari sul dark-web che altri malintenzionati potrebbero utilizzare per scopi illegali.

In riferimento al riscatto, sottolineano sempre le fonti, i pirati informatici non avrebbero al momento quantificato la loro richiesta in maniera esplicita anche se, in casi analoghi avvenuti in altri paesi, le richieste sarebbero passate da poche centinaia di migliaia fino a 10 milioni di euro. Nel frattempo gli investigatori della Polizia postale dell'Aquila a breve dovrebbero entrare in possesso di alcuni componenti elettronici installati su personal computer della Asl di Avezzano che sarebbero stati risparmiato dall'attacco hacker, con lo scopo appunto di effettuare dei confronti con i danni provocati da ignoti, iscritti sul registro degli indagati con le ipotesi di reato di accesso abusivo a sistemi informatici, danneggiamento e interruzione di pubblico servizio. Le informazioni verranno poi scambiate tra gli stessi investigatori dell'Aquila, con i colleghi della sede centrale di Roma e con la stessa Agenzia nazionale per la cyber sicurezza. Spetta invece al servizio tecnico interno della stessa Asl provvedere alla sistemazione dei server, al ripristino della rete internet.

Dal punto di vista investigativo, ci vorrà del tempo anche se le indagini portate avanti dalla Procura dell'Aquila, vanno avanti a ritmo incessante, mentre più lunghi potrebbero essere i tempi per ripristinare il sistema informatico; qualcuno ha ipotizzato anche un mese. Sulla vicenda è intervenuto anche il consigliere comunale Pd Stefano Palumbo che, parlando di «un fatto grave con ripercussioni sulle quotidiane prestazioni sanitarie che salteranno», ha evidenziato come «sia necessario che Biondi, in qualità di presidente del comitato ristretto dei sindaci e massima autorità sanitaria locale, insieme al direttore generale, venga al più presto a riferire in Consiglio comunale affinché sia fatta chiarezza su tutto e data massima diffusione».

Marcello Ianni

La sede della Asl dell'Aquila

Al casello di Tornimparte

Cocaina da Avezzano, scatta altro arresto

Pensava che uscendo dall'autostrada A24 al casello di Tornimparte di norma poco frequentato avesse potuto evitare un controllo; calcolo che si è rivelato errato. Gli agenti della Sezione narcotici della Squadra mobile, nell'ambito di servizi mirati volti a reprimere il dilagante fenomeno dello spaccio di droga, hanno arrestato in flagranza di reato, Ornella Nuccilli, 54 anni, dell'Aquila. La donna di ritorno da Avezzano è stata trovata in possesso di 21 grammi di cocaina, quantitativo non giustificabile per gli investigatori per un uso personale. Il controllo dopo che la donna a bordo della propria auto ha superato il casello di Tornimparte immettendosi sulla strada che porta allo stesso abitato. Su disposizione del Pm Roberta D'Avolio, la donna è stata arrestata. Nel corso dell'udienza di convalida la donna (assistita dall'avvocato Francesco Valentini) ha beneficiato della misura cautelare dell'obbligo di dimora in attesa della direttissima. Le indagini vanno avanti per appurare eventuali coinvolgimenti nello spaccio di cocaina e il canale di approvvigionamento della droga acquistata ad Avezzano.

M. I.

L'Aquila

■ L'Aquila - Viale Corrado IV, 50
■ Centralino Tel. 0862/61444-5-6
■ Fax Tel. 0862/22483
■ Pubblicità Tel. 0862/319301

■ e-mail: red.aquila@ilcentro.it

Al vostro fianco, da sempre.
PACINI
0862 24 593
www.onoranzefunebripacini.it

SANITÀ » QUARTO GIORNO DI CAOS E DISAGI

Ultimatum degli hacker alla Asl E l'emergenza finisce in Senato

È allarme sui dati: gli esperti confermano la diffusione di un referto medico con la richiesta di riscatto
Sistemi informatici ancora bloccati. Fina chiama in causa il ministro Schillaci: situazione molto grave

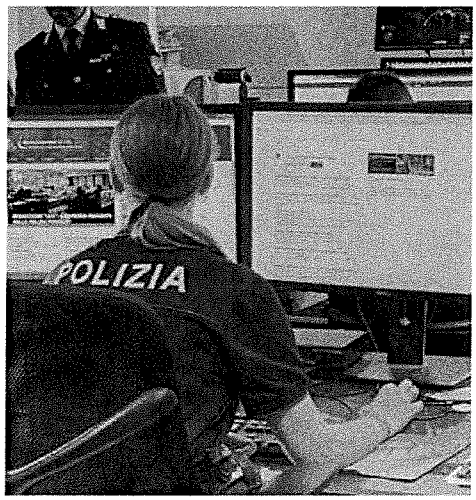
di Luca Tomassoni
L'AQUILA

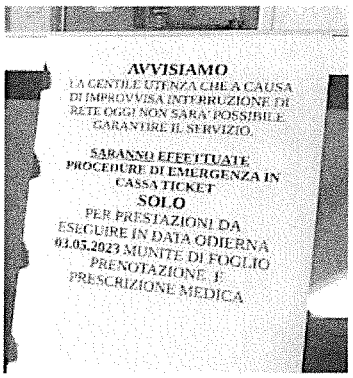
Il referto di un'ecografia, con tanto di nome della paziente, diffusa online: è la prima vera mossa pubblica dei pirati informatici che hanno messo sotto assedio la Asl aquilana, per far capire che fanno sul serio nel chiedere un riscatto all'azienda sanitaria. In altre parole: è un ultimatum. Che era già stato anticipato da un avvertimento: i pirati informatici del gruppo "Monti", nel rivendicare l'attacco "ransoware", avevano già parlato di 522 gigabyte di documenti prelevati dall'archivio digitale e minacciato direttamente di diffondere dati sui sieropositivi della provincia. Mentre la polizia postale indaga, è la rete internazionale di piattaforme web di esperti di cybersicurezza a confermare la diffusione del documento, avvalorando l'allarme sui dati sensibili lanciato dal consigliere regionale del Movimento 5 Stelle **Giorgio Fedele**.

Nella sua battaglia per salvare i dati e sbloccare i sistemi informatici in tilt, la Asl, oltre che dagli agenti della Postale, è affiancata anche da una task force arrivata da Roma. E pure dalla Regione, che sta fornendo supporto e collaborazione attraverso il servizio Sanità digitale, con i tecnici e il dirigente **Camillo Odio**. Ieri si è tenuto un altro vertice all'Aquila, ma si lavora «senza soluzione di continuità». La Asl, nel frattempo, resta in silenzio.

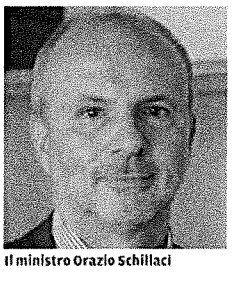
DISAGI SENZA FINE

Questo, mentre sembra ancora senza fine l'altra emergenza, quella più visibile: i disagi nelle strutture sanitarie, cominciati alle 4 del mattino di mercoledì, quando si è scoperto l'attacco hacker. Dall'ospedale dell'Aquila a quelli di Avezzano, Sulmona, Castel di Sangro, Pescina e Tagliacozzo, passando per i distretti sanitari e gli ambulatori: il blocco dei sistemi informatici produce il ritorno al cartaceo e di conseguenza code, rinvii e disservizi, che colpiscono soprattutto prenotazioni al Cup, esami e visite specialistiche. Tanto che giovedì la Asl ha rotto il silenzio con un avviso che segnalava lo stop alle visite dermatologiche prenotate per controlli nevi e per l'ambulatorio melanoma.





A destra l'avviso comparso allo sportello Cup dell'ospedale San Salvatore dell'Aquila A sinistra un'agente al lavoro: la polizia postale sta indagando sull'attacco hacker alla Asl mentre sono al lavoro anche esperti da Roma e dalla Regione


Il ministro Orazio Schillaci

» INDAGA LA POLIZIA POSTALE

Agenti al lavoro insieme a un gruppo di tecnici da Roma e dalla Regione

» IL TRIBUNALE DEL MALATO:

«Inondati di telefonate Problemi soprattutto per l'assistenza domiciliare»

«Siamo inondati di telefonate degli utenti e come noi lo sono gli stessi operatori della Asl: in particolare, segnalo i disagi dei pazienti con l'assistenza domiciliare dell'Adi che dovevano ritirare i codici per gli esami», spiega **Catia Puglielli** del Tribunale del Malato, continuando: «È chiaro la Asl si trova in una situazione di forte difficoltà. Non essendo la prima volta che accade un attacco del genere, forse andava rafforzato il sistema di sicurezza informatica. Ma ora bisogna pensare all'emergenza, sperando che la situazione si risolva il primo possibile.

IL CASO IN PARLAMENTO

E ora il caso finisce in Parlamento. Ce lo porta il senatore abruzzese del Partito democratico **Michele Fina**, attraverso una interrogazione al ministro **Orazio Schillaci**. «Da giorni la Asl è alle prese con un attacco hacker che ha determinato il completo blocco dei servizi informatici con drammatiche ricadute su tutto il sistema sanitario del territorio», scrive, continuando: «Si registrano pesanti ripercussioni sull'attività medica e sui servizi ospedalieri e dei distretti. Gli operatori si trovano costretti a riportare con carta e penna ricoveri ed esami generando ritardi e disagi. Una situazione che pagheremo a lungo, visto che quando saranno ripristinati i servizi serviranno settimane per catalogare i dati mancanti. A questo si aggiunge il caso dei dati sottratti con informazioni sensibili di grande delicatezza. Una vicenda molto grave che è un vero e proprio caso nazionale e sul quale il silenzio della Regione è imbarazzante. Per questo sto presentando un'interrogazione al ministro della Sanità al fine di conoscere con urgenza quali azioni sono state attivate per porre rimedio alla situazione, quali e quanti i dati sensibili trafugati e quali risorse possono essere subito impiegate per mettere in sicurezza sistemi evidentemente vulnerabili e obsoleti».

L'ALTRO CASO

Santangelo: «Anomalie nel budget all'ex Onpi»


Roberto Santangelo

L'AQUILA

Mentre la Asl è immersa nel caos dell'attacco hacker, scoppia un altro caso, che riguarda la residenza per anziani nell'ex Onpi dell'Aquila e in particolare «anomalie nell'accredito strutture regionali».

A segnalarlo è il vicepresidente del consiglio regionale **Roberto Santangelo**, che in una stringata nota spiega: «Sono venuto a conoscenza di difformità per quanto riguarda il budget destinato all'ex Onpi dell'Aquila, importante residenza pubblica per gli anziani e che svolge un ruolo cardine nell'assistere quanti non sono più autosufficienti. Ho prontamente interessato l'assessore regionale alla Salute, **Nicoletta Verì**, che si è immediatamente adoperata presso gli uffici regionali per capire qual è la soluzione migliore per risolvere questo problema. Seguirò personalmente la questione che investe un settore della nostra società particolarmente delicato».

Santangelo non ha però diffuso ulteriori dettagli sulla vicenda dell'accredito per la residenza per anziani, lasciando il compito alla giunta regionale.

L'Aquila

■ L'Aquila - Viale Corrado IV, 50
■ Centralino Tel. 0862/61444-5-6
■ Fax Tel. 0862/22483
■ Pubblicità Tel. 0862/319301

■ e-mail: red.aquila@ilcentro.it

Al vostro fianco, da sempre.
PACINI
0862 24 593
www.onoranzefunebripacini.it

ASL SOTTO ATTACCO » IL NUOVO AVVERTIMENTO

Gli hacker minacciano i medici: pubblichiamo anche i vostri dati

La banda di cybercriminali torna a chiedere il riscatto, oltre ai pazienti nel mirino pure i dipendenti
La polizia postale tenta di fermarli. Sistemi ancora bloccati: in ospedali e uffici rispolverati i fax

di Luca Tomassoni
L'AQUILA

Gli hacker aumentano la pressione sulla Asl aquilana. Ieri un nuovo avvertimento è apparso sul sito internet della gang "Ramsomware Monti" che da quattro giorni tiene sotto assedio l'azienda sanitaria chiedendo un riscatto per liberare l'archivio digitale e il sistema informatico. Sotto minaccia ora ci sono anche le migliaia di dipendenti, oltre ai pazienti con condizioni mediche più delicate. Nel frattempo continuano le enormi difficoltà per gli operatori e i disservizi per gli utenti: con il sistema informatico bloccato, si è tornati al cartaceo e all'utilizzo dei fax, fattore che ha mandato nel caos interi settori della Asl, a partire dal sistema per la prenotazione di visite ed esami. E l'azienda continua a restare in silenzio.

A sinistra la polizia postale al lavoro contro gli hacker Qui accanto il personale sanitario in ospedale: minacciata la diffusione anche dei dati dei dipendenti

LA NUOVA MINACCIA

I cybercriminali hanno già diffuso il referto medico di un'ecografia, con tanto di nome della paziente. Ora lanciano nuove minacce, disegnando tre step consecutivi di pubblicazione dei documenti. Il primo, immediato: «Adesso siamo pronti a pubblicare i seguenti dati nel nostro blog: dati personali dei dipendenti dell'organizzazione, compreso residenza, telefono, e-mail e codice fiscale; informazioni amministrative della sezione "Controllo di gestione"; dati legali, inclusi pronunciamenti giudiziari, protocolli, ecc.; 15 documenti casuali dal server dell'organizzazione; 15 documenti casuali successivi al 2022 dal sistema di archivio. Oltre a ciò, perché non abbiate dubbi che siamo in possesso i dati medici dei vostri pazienti, pubblicheremo parte dei documenti del monitoraggio della loro pressione sanguigna».

Il secondo step: «Se le nostre richieste non saranno accolte, allora saremo costretti a pubblicare il resto dei dati medici sul monitoraggio della pressione dei pazienti, oltre ad altri dati medici come diagnosi e trattamenti prescritti nelle aree della Fisiopatologia e dell'Ostetricia, con altri 50 documenti casuali».

Il terzo step: «Se nemmeno dopo arriveremo a un accordo, pubblicheremo i seguenti dati: dati medici di pazienti affetti da Hiv, oncologici e dei neonati, oltre alle informazioni sulla mortalità dei bimbi nelle vostre strutture; il resto dei documenti dal server e dall'archivio; i dati conservati nel backup del sistema Dedalus Dnlab. Ricordate che possediamo più di 500 Gigabyte di dati della vostra organizzazione».

LA TASK FORCE E IL RISCATTO

A combattere gli hacker in prima linea c'è una task force di esperti, che parlando di «situazione molto grave». Schierati, oltre ai tecnici dell'azienda sanitaria e a quelli di supporto della Regione, anche e soprattutto gli agenti della polizia postale. In particolare del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) di Roma e del Centro operativo sicurezza cibernetica (Cosc) di Pescara. Mentre è stata aperta una inchiesta – ma risalire ai cybercriminali sembra davvero impresa difficilissima – gli esperti stanno tentando di sbloccare i sistemi informatici della Asl e di bonificare i file criptati. Operazioni, queste, che potrebbero richiedere settimane, se non addirittura mesi prima di un ritorno alla normalità.

La richiesta di riscatto è arrivata, ma non sarebbe stata ancora "aperta" e letta: il timore è che appena verrà cliccato il link inviato dal gruppo di hacker Monti, si avvierà un conto alla rovescia. Che in questi casi è di poche ore, forse intorno ai tre giorni.

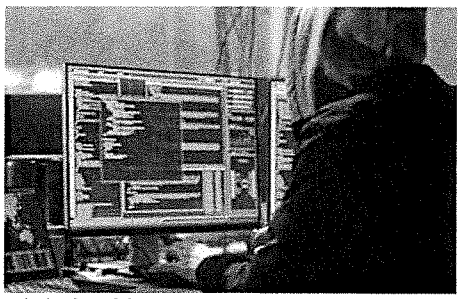
L'antivirus pagato 40mila euro un anno fa

Dopo lo scoppio della guerra in Ucraina arrivò la decisione di sostituire il vecchio programma russo

L'AQUILA

Solo un anno fa la Asl aquilana aveva cambiato il suo sistema di sicurezza informatica. E lo aveva fatto con «carattere di urgenza», per una motivazione che oggi suona come una beffa: si temevano attacchi informatici dai russi, visto il deteriorarsi dei rapporti tra Italia e Mosca a causa dello scoppio della guerra in Ucraina. Russo era infatti il vecchio antivirus utilizzato dalla Asl.

«Questa Asl si avvale di una infrastruttura informatica complessa, divenuta nel tempo elemento determinante in tutte le aree produttive aziendali, tanto in quelle prettamente sanitarie, quanto in quelle amministrative e logistiche», si leggeva nell'atto di acquisto del nuovo antivirus, pagato poco meno di 40mila euro, «in linea con quanto indicato dall'Agenzia per l'Italia digitale, negli anni sono stati realizzati continui interventi sui sistemi informativi aziendali volti a potenziare e attualizzare tali strumenti nelle componenti hardware e in quelle software; in relazione alle esigenze di sicurezza dei sistemi informativi aziendali, con particolare riguardo alle componenti software sia sistemistiche e sia applicative, questa Asl si è dotata di prodotti software specifici che, nel tempo, hanno richiesto un continuo aggiornamento per garantirne l'efficacia: nel 2020 è stato acquisito un software antivirus di produzione russa. Il Servizio sistemi informativi ha richiesto la fornitura di un nuovo software antivirus aziendale, in sostituzione di quello attualmente in utilizzo. In tale richiesta è stato sottolineato il carattere di urgenza della fornitura, in relazione ai possibili rischi derivanti da attacchi informatici». *(l.t.)*



Un hacker davanti al computer

Partita la staffetta tra sport e lotta al cancro

Al via dall'Aquila la Run 4 Hope: da oggi si corre lungo la costa teramana, poi Lanciano e Pescara

Un momento della partenza dal Parco del Castello dell'Aquila

di Fabio Iuliano
L'AQUILA

È partita dall'Aquila, alle undici in punto in contemporanea nazionale, la staffetta Run 4 Hope, la staffetta di solidarietà per sostenere la ricerca. I fondi raccolti saranno destinati all'Aire per la lotta contro i tumori femminili. Un'iniziativa che si propone come connubio perfetto tra sport e ricerca costituita a un giro podistico solidale che, regione per regione, attraversa tutto il Paese. Coinvolti a livello nazionale 40.000 podisti grazie all'adesione di oltre 400 associazioni sportive, 41 reparti tra Esercito italiano, Marina militare ed Aeronautica militare, oltre a centinaia di individualisti che correranno in "modalità virtual". Si stima che i vari testimoni percorreranno complessivamente oltre 6mila chilometri toccando quasi tutte le province della penisola. In Abruzzo, la tappa di apertura ha raggiunto Montorio al Vomano. Oggi si corre alla volta della costa teramana. La terza tappa è prevista da Martinsicuro a Silvi nella giornata di domani, la quarta da Silvi a Lanciano passando per Pescara martedì 9, la quinta da Lanciano a Paleno. Poi il rientro nella provincia dell'Aquila per la conclusione ad Avezzano, domenica 14. L'organizzazione è a cura di Atletica Abruzzo L'Aquila, in collaborazione con l'Asd Usa Sporting Avezzano. Alla partenza di Run4Hope al Parco del Castello c'erano anche alcuni rappresentanti dell'Esercito, in forze al comando militare esercito Abruzzo e Molise. A dare il via, il presidente dell'Asd Atletica Abruzzo L'Aquila Valter Paro, dall'assessore comunale allo Sport **Vito Colonna**, il presidente del comitato esecutivo di "L'Aquila Rinasce con lo Sport" **Francesco Bizzarri**, il presidente del comitato regionale Fidal **Massimo Pompei**, oltre a **Marco Iovinelli**, comandante del Comando militare Esercito Abruzzo. A dare il via anche **Eliseo Irti** in rappresentanza dell'Aire, la fondazione italiana per la ricerca sul Cancro. La manifestazione rientra nel calendario di eventi "Rinasci con lo sport - promuovere L'Aquila con lo sport 2023", è organizzata in Abruzzo dall'Asd Atletica Abruzzo L'Aquila in collaborazione con l'Esercito Italiano che ha partecipato in maniera attiva, sia con alcuni atleti, sia nell'allestimento degli stand. Testimonial della staffetta è **Margherita Magnani**, ex campionessa italiana di mezzo fondo che ha partecipato alla conferenza di presentazione.