AbruzzoWeb
Tutte le notizie d'Abruzzo a portata di click

HACKER ASL L'AQUILA: AZIONE, "GESTIONE DISASTROSA, SUBITO DIMISSIONI DEI VERTICI AZIENDALI"

8 Maggio 2023



L'AQUILA – "Se a destra (che governa) e a sinistra (che ha governato) nessuno fiata, noi siamo liberi da condizionamenti e restiamo esclusivamente dalla parte dei cittadini che assistono sgomenti a questo disastro, non dovendo tutelare né amici né amici degli amici. Anche se da soli, perché nessuno al di là di qualche protesta di facciata va oltre, noi lo chiediamo a gran voce: Dimissioni di questo vertice della Asl al più presto! Così non si può più andare avanti".

Anche Azione, con Giorgio Ciocca membro direzione comunale dell'Aquila ed esperto nella protezione dati, ed Enrico Verini, consigliere comunale di Azione L' Aquila, interviene della drammatica emergenza negli ospedali e presidi sanitari della Asl provinciale dell'Aquila, dove i servizi sanitari sono in buona parte in ginocchio, e riservati ai casi più urgenti, con documenti scritti e consegnati a mano, e addirittura con il ritorno ai fax. Questo a seguito del micidiale all'attacco, partito da qualche

parte del mondo, dei famigerati hacker della Ramsomware Monti, che hanno violato e messo fuori uso i server aziendali, riuscendo a rubare anche 500 gigabyte di dati sensibili , tra referti, analisi, cartelle cliniche, esami.

Chiedendo un riscatto per non renderli pubblici. E arrivano a chiedere le dimissioni del manager in quota centrodestra, Ferdinando Romano.

“Si poteva fare qualcosa (anche di più) per evitare tutto questo? Quali sono le norme tecniche e legislative che questi settori devono seguire per arginare il fenomeno del ransomware?” Ebbene la risposta non potrà che essere un sì, si poteva fare di più”, spiegano nella lunga e articolata nota.

LA NOTA COMPLETA

Un risveglio amaro dalle festività del 25 Aprile e del 1 Maggio per i cittadini del comprensorio aquilano che avevano pianificato e prenotato una visita specialistica od ambulatoriale presso i servizi della ASL1 dell’Aquila-Avezzano-Sulmona, perché come un fulmine a ciel sereno (ma non per gli esperti del settore Data Protection, GDPR e Privacy, che conoscono il fenomeno che accade specialmente durante le festività) coloro che si sono presentati presso gli sportelli del CUP di L’Aquila, si sono visti negare il loro diritto alla salute, perché i sistemi informatici dalla mattina del 3 maggio erano bloccati.

Dalle prime sembrava essere un mero blocco della comunicazione di rete ed internet, ma da subito si è compreso che era accaduto quello che recentemente è diventato l’incubo di ogni amministratore pubblico e/o del privato e del responsabile dei sistemi informatici: un ransomware.

Assistiamo, ormai sembra “inermi”, a quella che è diventata la sistematica forma di estorsione economica a distanza verso Enti ed aziende denominata “ricatto ransomware”, in base al quale determinati soggetti od organizzazioni criminali, dalle più svariate parti del globo, sono in grado di iniettare nei sistemi informatici attaccati, un determinato virus informatico, appunto il “ransomware” in grado di criptare (rendere inaccessibile ed illeggibile) la maggior parte dei file presenti nei computer, file necessari alla azienda per lavorare.

La caratteristica di questa criptazione è che la chiave di decriptazione per riaccedere ai file è generata e conservata appunto dagli stessi “criminali informatici” (non chiamiamoli hacker), i quali lasciano nei computer infetti le istruzioni e le coordinate destinate agli amministratori per pagare entro una determinata data un riscatto economico elevato da versare su conti legati a monete virtuali (es. bitcoin), quindi irrintracciabili normalmente dalle Autorità di Polizia e Giudiziarie.

Adesso tralasciando ulteriori evoluzioni dei prossimi giorni, che si indirizzeranno nel ripristinare i sistemi ed anche nell’accertare, sia all’interno della ASL1 che all’esterno, la situazione per tramite delle Autorità chiamate, obbligatoriamente, ad investigare ed accertare quanto accaduto (Garante Protezione Dati Personali conosciuto come anche Garante Privacy ed il CNAIPIC il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche) la domanda che non possiamo evitare di farci è:” si poteva fare qualcosa (anche di più) per evitare tutto questo? Quali sono le norme tecniche e legislative che questi settori devono seguire per arginare il fenomeno del ransomware?”

Ebbene la risposta non potrà che essere un “SI”, si poteva fare di più.

La soluzione, e prescrizione conseguente, potrebbe essere evidenziata e trovarsi all’esito di quelle che quasi sicuramente saranno le attività ispettive delle Autorità preposte, trovandosi la ASL nella situazione prevista dal Regolamento UE 2016/679 GDPR, noto come Regolamento sul Trattamento dei Dati Personali, ovvero nella situazione prevista dagli articoli del GDPR n.32 (Sicurezza del trattamento), n.33 (Notifica di una violazione dei dati personali all’Autorità di controllo), n.34 (Comunicazione di una violazione dei dati personali all’interessato).

Ricordiamo che si parla di 522GB di dati esfiltrati dalle infrastrutture IT dell’Azienda Sanitaria e, nonostante il tentativo di minimizzazione della Asl, pare che “molteplici vulnerabilità hanno consentito il download di dati persino sui pazienti sieropositivi”.

Pertanto si tratta di dati ultra sensibili dei pazienti della ASL che possono essere pubblicati dalla cybergang e riversati nel darkweb per porre ulteriori forme di estorsione, magari individuali, verso soggetti di cui si hanno informazioni protette appunto da quella che dovrebbe essere un “legittimo diritto alla privacy”

Oltre quello che può essere lo sconcerto iniziale per una situazione in cui purtroppo, come cittadini, siamo in parte meri spettatori non avendo strumenti diretti da poter agire a difesa del nostro diritto a che i dati che ci rappresentato (se non il “reclamo” all’Autorità Garante od a quella Giudiziaria), nello specifico anche quelli più sensibili, vengano gestiti e conservati nelle modalità più adeguate e sicure possibili, e non possiamo non riflettere a che i nostri rappresentati politici ed

amministrativi locali prendano atto di quello che è “realmente accaduto” ed in primis si attivino per una pronta risoluzione ed anche una “dovuta spiegazione” alla cittadinanza (elettrice)

Ci rammarica che, da qualsiasi angolazione andiamo a valutare l’operato della dirigenza della nostra ASL, non possiamo che esprimere il totale disappunto per una gestione molto presuntuosa e nei fatti veramente lontanissima da quei livelli essenziali di prestazione, anche per la protezione dei dati, che dovrebbe offrire.

A breve forniremo altri incredibili circostanze di mal governo di cui i cittadini, spesso malati, sono vittime.

Se a destra (che governa) e a sinistra (che ha governato) nessuno fiata, noi siamo liberi da condizionamenti e restiamo esclusivamente dalla parte dei cittadini che assistono sgomenti a questo disastro, non dovendo tutelare né amici né amici degli amici.

Anche se da soli, perché nessuno al di là di qualche protesta di facciata va oltre, noi lo chiediamo a gran voce: Dimissioni di questo vertice della Asl al più presto! Così non si può più andare avanti.

© 2026 Abruzzo Web Enfasi srl - Quotidiano digitale registrato presso il Tribunale dell'Aquila con decreto n°501 del 2 settembre 2003
Iscrizione al ROC n. 26362 - P.IVA 01812420667
Direttore responsabile Berardo Santilli