**IL VIRUS DEL RISCATTO**
*Di Lucina Paternesi e Goffredo De Pascale*

**LUCINA PATERNESI FUORICAMPO**
È il tre dicembre del 2021 quando i sistemi informatici dell'azienda sanitaria 6 euganea vengono mandati in tilt da un attacco hacker: sospesi cup, prelievi, analisi, laboratori, liste d'attesa per fare tamponi e, ovviamente, anche gli hub vaccinali.

**ANDREA ATZORI - MEDICI CON L'AFRICA CUAMM**
Siamo stati informati dall'Asl di una problematica informatica, e un'ora dopo all'incirca abbiamo avuto un software sostitutivo e siamo ripartiti.

**LUCINA PATERNESI FUORICAMPO**
L'azienda sanitaria locale 6 copre più di cento comuni da nord a sud di Padova e una popolazione di quasi 1 milione di abitanti.

**RAFFAELLA MEGNA - FUNZIONE PUBBLICA CGIL PADOVA**
La gente che è stata qua 12 ore per fare a mano quello che normalmente fai col sistema computerizzato. C'è gente che veramente c'ha sputato il sangue, eh.

**LUCINA PATERNESI FUORICAMPO**
Risultano bloccati gli oltre settemila pc dislocati nei quattro ospedali. Viene creata una task force per ripristinare le attività più urgenti.

**INFERMIERA OSPEDALI RIUNITI PADOVA SUD – SCHIAVONIA (PD)**
Ci si doveva riorganizzare giorno per giorno. Quindi prendere il telefono, chiamare, accettare le persone che arrivavano perché non avendo gli elenchi di chi doveva fare la visita quel giorno.

**LUCINA PATERNESI**
Ma perché nessuno vuole parlare di questa storia?

**INFERMIERA OSPEDALI RIUNITI PADOVA SUD – SCHIAVONIA (PD)**
Purtroppo, siamo in una sorta di dittatura. Se la sanità ti dice che non devi parlare non devi parlare.

**SIGFRIDO RANUCCI IN STUDIO**
Bocche cucite perché nascondono un imbarazzo, c'è da nasconderlo… perché un milione di cittadini veneti all'improvviso non ha più potuto contare su un organizzatissimo modello sanitario. Il sistema informatico era bloccato, che cosa era successo? che un gruppo di hacker era riuscito a penetrare nei pc, di fatto, diventando l'amministratore di parte del sistema informatico sanitario. Sono riusciti a penetrare, hanno inserito un software malevolo, il ransomware, che ha di fatto cifrato i dati dei cittadini rendendoli inagibili e poi, prima però li aveva copiati e sfilati dal pc. Per non pubblicarli ha chiesto un riscatto di tre milioni di dollari. Ora, Report è venuta in possesso delle chat originali della trattativa. In esclusiva, la nostra Lucina Paternesi.

**LUCINA PATERNESI**
Quando se ne sono accorti alla Asl?

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
Immediatamente, subito, già 40 minuti che era successo l'attacco.

**LUCINA PATERNESI FUORICAMPO**
Grazie ai backup aggiornati l'azienda sanitaria non ha perso i dati, ma ha dovuto far fronte al ricatto degli hacker che minacciavano di pubblicare i dati sensibili dei pazienti. Gli ingegneri di Tg Soft si mettono sulle tracce del virus che ha infiltrato il sistema sanitario. Vanno su virustotal, una piattaforma molto usata dai ricercatori anti-virus.

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
Il software che noi abbiamo trovato genera delle istruzioni di riscatto che contiene una login e una password per accedere alla chat.

**LUCINA PATERNESI**
Quindi è sicuro che sia quello, non è un'ipotesi?

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
No no è proprio questa. Eccola qua, questa è la chat.

**LUCINA PATERNESI FUORICAMPO**
Gli analisti di Tg Soft hanno scoperto che qualche minuto dopo la mezzanotte del 3 dicembre qualcuno dentro l'Ulss inizia a chattare con i cybercriminali.

**CYBER CRIMINALI HIVE**
Salve e benvenuti su Hive. Come posso aiutarvi?

**ULSS 6**
Abbiamo necessità di decriptare i file, aiutateci per favore.

**CYBER CRIMINALI HIVE**
Per decriptare i file devi pagare 3 milioni e mezzo di dollari in bitcoin.

**ULSS 6**
È uno scherzo? Noi siamo un ente sanitario governativo.

**CYBER CRIMINALI HIVE**
Sappiamo chi siete.

**ULSS 6**
Dimmi quanto vuoi realmente e possiamo discutere.

**CYBER CRIMINALI HIVE**
Posso farti uno sconto di cinquecentomila dollari.

**ULSS 6**
Dovremmo pagare 3 milioni di dollari per i dati? Siete folli!

**CYBER CRIMINALI HIVE**
Non mi insultare altrimenti chiudo la conversazione immediatamente.

**LUCINA PATERNESI FUORICAMPO**
Dunque, qualcuno ha provato a contrattare con i criminali. Ha chiesto anche lo sconto, ma poi accade l'impensabile.

**ULSS 6**

Prima puoi baciarmi il c*** e poi dare l'indirizzo di tua madre verrò a trovarla. Cercate un'altra occupazione stupidi bastardi.

**CYBER CRIMINALI HIVE**
Se non ci sarà il pagamento renderemo tutti i file esfiltrati pubblici.

**LUCINA PATERNESI FUORICAMPO**
Dalla direzione dell'Ulss smentiscono le trattative con i cybercriminali. Ma allora chi parlava con gli hacker?

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
Io sono convinto, e lo spero, che i dirigenti della Asl non sappiano, non abbiano autorizzato questo tipo di trattativa perché se no sarebbe una follia.

**LUCINA PATERNESI**
Ma perché c'è un manuale per come si conducono le trattative?

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
Beh, non c'è un manuale ma c'è un buonsenso. Quando tu hai in mano i dati di, come ha detto lei, un milione di persone forse bisognerebbe andare coi piedi di ferro, di piombo… insomma.

**LUCINA PATERNESI FUORICAMPO**
Avere un backup aggiornato consente di non perdere tutti i dati. Ma questo non basta a fermare le minacce e un mese dopo, il 1 gennaio, entra in gioco un secondo gruppo di cyber criminali: Lockbit. Parte il countdown: se l'Ulss non paga verranno pubblicati tutti i dati trafugati dai computer.

**LUCA ZAIA - PRESIDENTE REGIONE VENETO CONF. STAMPA 17/01/22**
Non abbiamo pagato il riscatto, quindi mi spiace hanno anche lavorato tanto per niente. Che poi io non so se sta roba è una roba di una persona fisica di uno che è lì che fa ste robe, o se è proprio questione di macchine, di algoritmi, di intelligenza artificiale. Non ho ben capito, è un mondo che non conosciamo però è un mondo pericolosissimo.

**GIANFRANCO TONELLO - ANALISTA MALWARE E FONDATORE TG SOFT**
Arriva il giorno dell'ultimatum, succede alla sera verso le 22 che Lockbit non aspetta la scadenza pubblica e mette online i dati.

**LUCINA PATERNESI FUORICAMPO**
Finiscono online oltre 9mila file, divisi in 51 cartelle. Documenti amministrativi, verbali, regolamenti, disposizioni interne, ma anche risultati dei tamponi, certificati medici, referti specialistici, diagnosi, denunce da aggressione e persino i nomi e i numeri di telefono dei pazienti oncologici del Veneto.

**CESARE BUREI - BROKER ASSICURATIVO**
Quando ci sono stati i breach sulle cartelle cliniche, son stati valutati, a cartella clinica, sui mille dollari.

**LUCINA PATERNESI**
Sono tutti di un ospedale, ci sono gli elenchi dei pazienti oncologici.

**CESARE BUREI - BROKER ASSICURATIVO**

Documenti d'identità completi, diplomi, quindi io potrei sostituirmi a delle persone in toto, crearmi un'identità digitale completa, con tanto di scansione del documento fronte retro a colori. Ci sono i moduli per ordinare i vaccini, le etichette, i codici di ordine. Conosco le procedure interne, bene. Voglio infilarmi in una procedura sanitaria. Ti studio, ti ho dato materiale per studiarmi.

**LUCINA PATERNESI FUORICAMPO**
Sulla vicenda il Garante per la privacy ha aperto un'istruttoria per capire se è stato fatto il possibile per impedire la divulgazione online di dati sensibili. Rischiano una multa fino a 10 milioni di euro.

**INFERMIERA OSPEDALI RIUNITI PADOVA SUD – SCHIAVONIA (PD)**
Adesso hanno iniziato a cambiare i computer, hanno iniziato ad aggiornare il sistema, perché potrebbe anche esser stato un dipendente involontariamente ad aver messo qualcosa su un computer, ad aver aperto la porta, cioè chi lo sa?

**LUCINA PATERNESI SPOSTATO QUI**
Ma secondo lei ci possono essere delle responsabilità da parte dell'azienda per quello che è successo?

**INFERMIERA OSPEDALI RIUNITI PADOVA SUD – SCHIAVONIA (PD)**
Ma sicuramente sì. Addirittura alcuni computer erano all'età di Windows 8 dove non si potevano fare più aggiornamenti.

**LUCINA PATERNESI FUORICAMPO**
Ma a chi toccava mettere in sicurezza le reti informatiche della sanità veneta?
Secondo la stessa legge che l'ha istituita nel 2016, Azienda Zero, società in house della Regione Veneto, aveva tra i suoi compiti la gestione delle infrastrutture tecnologiche, dei sistemi informativi e dei dati degli enti del servizio sanitario regionale.

**ALESSANDRO ZAN - DEPUTATO PD**
Questo non è stato fatto e le singole Ulss hanno dovuto continuare con i loro sistemi informatici ma che non erano assolutamente adeguati per contrastare un attacco hacker come quello che c'è stato lo scorso 3 dicembre all'Ulss 6 di Padova.

**LUCINA PATERNESI FUORICAMPO**
Dai verbali riservati della commissione sanità d'inizio marzo emerge con chiarezza che negli ospedali mancavano le più basilari forme di protezione, come la doppia autenticazione per aprire la posta elettronica e i corsi di formazione per sanitari e medici.

**ALESSANDRO ZAN - DEPUTATO PD**
Oggi è una scatola quasi vuota, perché fa solo bandi e appalti. Le Ulss sono state svuotate di competenza, ma dall'altra parte non c'è stata ad esempio la creazione di un team di uno staff in Azienda Zero che potesse dare quel sostegno da un punto di vista informatico e della protezione dei dati.

**LUCINA PATERNESI FUORICAMPO**
Oltre il danno, la beffa. Solo per bonificare e sostituire i computer compromessi e dotarsi di una consulenza da parte di una società esterna di cyber Security, nei due mesi successivi l'attacco l'Ulss 6 ha speso in emergenza quasi 1 milione di euro.

**ROBERTO BALDONI - DIRETTORE AGENZIA CYBER NAZIONALE**

Noi siamo entrati in contatto con l'Ulss6 di Padova proprio per cercare di aiutarla a superare l'evento che hanno subito, credo che faccia parte della Nis.

**LUCINA PATERNESI FUORICAMPO**
La Nis è la normativa europea che prevede l'obbligo di creare un livello comune di sicurezza delle reti. Sono tenuti a rispettare gli obblighi imposti da questa normativa anche gli enti pubblici che offrono servizi essenziali sanitari, proprio come la Ulss6 di Padova. Il ruolo di controllo è in capo alle Regioni, che possono anche sanzionare chi non rispetta i requisiti.

**LUCINA PATERNESI**
La Regione che fa, sanziona sé stessa?

**ROBERTO BALDONI - DIRETTORE AGENZIA CYBER NAZIONALE**
Esattamente. Ma infatti è un sistema che non stava in piedi.

**LUCINA PATERNESI FUORICAMPO**
La Regione Veneto, dunque, avrebbe prima dovuto garantire la sicurezza, poi controllare e addirittura arrivare a sanzionare sé stessa nel caso in cui l'attacco hacker si fosse verificato per sua inadempienza.

**LUCINA PATERNESI**
É mai stato sanzionato qualcuno ad oggi?

**ROBERTO BALDONI - DIRETTORE AGENZIA CYBER NAZIONALE**
Francamente non credo.

**SIGFRIDO RANUCCI IN STUDIO**

Sarà l'Agenzia cyber nazionale a controllare e verificare se ci sono i requisiti e anche a sanzionare in caso di inadempienza. Questo per togliere alle regioni l'imbarazzo di decidere se sanzionare o meno se stesse. Però la Ulss padovana con noi non ha voluto parlare. Ci ha scritto e ci dice:" è stata vittima di un crimine e sta dando il massimo del supporto agli utenti coinvolti, e che è sempre rimasta in possesso dei dati perché aveva il backup". Evviva, Dio. Però su questa vicenda sta indagando la Direzione distrettuale antimafia di Venezia e anche il Garante della privacy, ovviamente per le parti che competono sulla responsabilità della violazione a danno degli utenti. Attacchi hacker ci sono stati anche ai danni del sistema informatico sanitario della Lombardia, della Campania e anche del Lazio. Ed è per questo che continueremo a seguire questa vicenda perché intorno ai dati sanitari, ci sono interessi pazzeschi, a partire da quelli di un Paese che si sta preparando alla guerra.