Attacco informatico alla multinazionale JBS, in Australia produzione ferma e dipendenti a casa

La filiale statunitense del colosso agroalimentare brasiliano **JBS**, uno dei leader mondiali nel settore della carne, ha annunciato ieri sera di essere stata vittima di un "attacco informatico organizzato".

"JBS Usa ha scoperto di essere stata l'obiettivo di un attacco organizzato alla sicurezza informatica che ha colpito molti dei server su cui si basa il suo sistema informatico in Nord America e Australia", ha affermato la società in una nota senza specificare la natura di tale attacco.

"Tutti i sistemi interessati sono stati fermati e le autorità avvertite, ha affermato Jbs Usa aggiungendo che i suoi sistemi di backup non sono stati interessati dall'accaduto. *"In questa fase, l'azienda non è a conoscenza di alcun uso improprio dei dati relativi ai propri clienti, fornitori o dipendenti derivante da questa situazione",* ha aggiunto Jbs Usa avvertendo tuttavia che le transazioni con i propri clienti e fornitori potrebbero essere "rallentate".

JBS, specializzata in prodotti di manzo, pollo e maiale, è una delle più grandi aziende alimentari al mondo. Oltre che in Brasile e negli altri Paesi dell'America Latina, è presente in Stati Uniti, Canada, Australia, Nuova Zelanda e Regno Unito.

#BREAKING US branch of meat-packing Giant JBS says it was

> *hacked pic.twitter.com/A5EMW6mnaR*
>
> *— AFP News Agency (@AFP) June 1, 2021*

In Australia produzione ferma e dipendenti a casa. Il ministro Littleproud: "ci vorranno giorni affinché la produzione riprenda"

In Australia la situazione è critica. In una dichiarazione all'AFP il ministro dell'agricoltura australiano **David Littleproud** ha affermato di essere *"il governo australiano e la polizia federale stanno lavorando con JBS per risolvere il problema e trovare i responsabili dell'attacco. Ci vorranno giorni affinché la produzione riprenda".*

Secondo un rappresentante sindacale intervistato dall'**Associated France Presse** (**AFP**), le strutture australiane dell'azienda, paralizzate dall'attacco, hanno lasciato 10mila lavoratori a casa.

L'attacco informatico alla multinazionale, con la conseguente chiusura della produzione, potrebbe far aumentare i prezzi nella carne in Australia e in Nord America come si è visto recentemente con l'aumento del prezzo della benzina negli Usa in seguito l'hack del Colonial Pipeline.

Colonial Pipeline: il governo degli Stati Uniti prende provvedimenti

L'hack arriva meno di un mese dopo che un grave attacco informatico ha bloccato la rete Colonial Pipeline, l'oleodotto che trasporta circa il 45% del carburante consumato sulla costa orientale degli Stati Uniti.

Le vulnerabilità informatiche degli oleodotti statunitensi hanno portato il governo federale la scorsa settimana a imporre per la prima volta requisiti di sicurezza informatica agli oleodotti.

Le nuove regole, imposte dal Department of Homeland Security, richiedono agli operatori delle condutture di designare un coordinatore della sicurezza informatica che deve essere disponibile in ogni momento e di segnalare gli incidenti informatici alla Cybersecurity and Infrastructure Security Agency.

https://www.key4biz.it/attacco-informatico-alla-multinazionale-jbs-in-australia-produzione-ferma-e-dipendenti-a-casa/362868/

Cyberspionaggio dell'Nsa a danno di politici Ue, tra cui la Merkel. Snowden tira in ballo Biden

Ancora una volta si torna a parlare di **Nsa**, l'Agenzia per la sicurezza nazionale degli Stati Uniti, e di attività di **cyberspionaggio** ai danni di funzionari e politici europei di alto profilo, tra cui parlamentari francesi, norvegesi, svedesi e tedeschi, tra cui nomi di grande spicco istituzionale.

In Germani, ad esempio, risultano oggetto di sorveglianza

illecita politici come la cancelliera **Angela Merkel**, ma anche l'ex presidente **Frank-Walter Steinmeier** e l'ex ministro delle Finanze **Peer Steinbrueck**.

L'Nsa ha spiato i politici europei

Per arrivare a questo, si legge su diversi articoli apparsi oggi sui media internazionali, tra cui BBC e Politico, **l'Nsa si è fatta aiutare dai servizi segreti della Danimarca o almeno da quelli "deviati"** (come li chiama da sempre la stampa italiana).

L'emittente pubblica danese **DR** (Danmarks Radio) ha rivelato il caso, relativo ad un'indagine interna sempre dei servizi del 2015, mentre il dossier è nelle mani anche di altri media dei Paesi coinvolti dall'azione di spionaggio, come *Le Monde* per la Francia, la *'Suddeutsche Zeitung'* e i canali tv tedeschi Ndr, Wdr, svedese Svt e norvegese Nrk.

La Danimarca è terminal di cavi internet sottomarini da e per Norvegia, Francia, Svezia e Germania, motivo per cui l'Nsa ha effettuato forti pressioni proprio sull'Agenzia di Intelligence della Difesa danese (FE) per portare avanti l'azione di cyberspionaggio.

Le reazioni

Il ministro della Difesa danese, **Trine Bramsen**, ha riferito alla DR che "*le intercettazioni sistematiche di Paesi alleati sono inaccettabili*".

"*E' grottesco essere spiati dai servizi di intelligence di un Paese amico, lo ritengo assolutamente scandaloso*", ha commentato Steinbrueck all'emittente tedesca ARD.

Il ministro della Difesa svedese **Peter Hultqvist** ha dichiarato all'emittente svedese SV "*di aver chiesto spiegazioni alla*

Danimarca su quanto accaduto”, mentre il collega norvegese, **Frank Bakke-Jensen**, ha detto di prendere molto sul serio la faccenda.

I fatti dovrebbero risalire al periodo 2012-2014, durante i quali l’attuale Presidente degli Stati Uniti**, Joe Biden**, era vicepresidente sotto l’amministrazione guidata da **Barak Obama**.

“Biden non poteva non sapere“

Cosa che secondo **Edward Snowden** fa di Biden persona a conoscenza dei fatti. Snowden è l’informatico ex collaboratore dell’Nsa che per primo nel 2013 denunciò al mondo la sorveglianza di massa digitale messa in pratica dall’Agenzia americana, che passò alla storia con il nome di “*Datagate*”.

L’anno scorso la Corte di Appello USA ha riconosciuto Snowden innocente dalle accuse di alto tradimento (l’ex Presidente USA, **Donald Trump**, non esitò a dichiarare Snowden degno di una condanna a morte), ribandendo l’illegalità invece delle azioni dell’Nsa.

https://www.key4biz.it/cyberspionaggio-dellnsa-a-danno-di-politici-ue-tra-cui-la-merkel-snowden-tira-in-ballo-biden/362728/

Sanità irlandese sotto cyber attacco, sconvolto il sistema delle prenotazioni. Il

Premier Martin: “Atto atroce”

Un attacco “*devastante e catastrofico*”, è stato definito quello portato al sistema sanitario irlandese nei giorni scorsi. L’amministratore delegato dell’Health Service Executive (HSE), **Paul Reid**, ha parlato chiaramente di “*attacco sconvolgente*” ai sistemi informatici sanitari e ospedalieri del Paese, di un’aggressione insensibile agli operatori sanitari che lavorano ogni giorno per proteggere la salute dei cittadini.

Da una settimana **l’Hse ha dovuto disattivare tutti i suoi sistemi informatici e le reti interne** per provare a contenere i danni e soprattutto difendere in ogni modo i dati sanitari e sensibili dei pazienti e delle strutture.

Le conseguenze dirette dell’attacco

La prima conseguenza è che **il sistema di gestione degli appuntamenti e delle visite è saltato**, cosa che ha costretto gli operatori ha **riprendere in mano carta e penna** per venire incontro alle esigenze dei cittadini.

I servizi ambulatoriali sono stati fortemente compromessi dall’attacco e la gran parte è stata cancellata.

i tecnici e gli informatici inviati dal Governo sono al lavoro da giorni, senza sosta, è stato spiegato in un briefing ieri, secondo quanto riportato in un articolo della BBC, ma ci sono da controllare più di 2.000 sistemi informatici utilizzati dall’Hse e oltre 4.500 server.Documenti online non accessibili

Non è stato possibile accedere a molte cartelle cliniche elettroniche o fascicoli sanitari online, per portare avanti

le analisi e le visite più delicate si è proceduto con moduli cartacei, compilati a mano e portati di corsa ad altri laboratori, come accadeva decenni fa, perché la rete non supportava nessuna attività di condivisione online dei dati (proprio per la disattivazione dei sistemi informatici e di rete per contenere l'attacco).

Una situazione considerata ancora molto critica, quindi, perché tornare a carta e penna, alle consegne "a mano" delle richieste di analisi ai laboratori e dei risultati ai medici e ai pazienti, è un danno al livello di qualità dei servizi, delle terapie e delle cure, perché si perde troppo tempo e soprattutto torna di nuovo alla ribalta il **fattore "errore umano", che aumenta notevolmente in queste situazioni**.

Le reazioni del Governo

Della faccenda si sta occupando anche il Governo di Dublino. Secondo il Primo ministro irlandese o "*Taoiseach*", **Micheál Martin**, quello contro l'Hse è "*un atto atroce*", un attacco diretto contro il popolo irlandese.

"*Per questo abbiamo deciso di aumentare le difese informatiche dell'intero Paese, delle sue infrastrutture critiche e dei sistemi di base, con una revisione continua degli standard di sicurezza di tutte le agenzie governative*", ha affermato Martin.

"*Fortunatamente i dati sottratti dai cyber criminali non sono state condivise in rete*", ha commentato su RTE il ministro irlandese delle Comunicazioni, **Eamon Ryan**, definendo comunque il comportamento degli hacker come "*profondamente deplorevole*".

Le indagini del Cyber □□Crime

Bureau

L’indagine giudiziaria in corso è guidata dal **Garda National Cyber Crime Bureau**, in collaborazione con il **National Cyber Security Center** e l’Hse.

Un portavoce del Dipartimento per l’ambiente, il clima e le comunicazioni, che include il National Cyber Security Center, nonostante le parole del ministro Ryan, ha affermato che esiste ancora un elevato rischio “*che i dati personali e sanitari dei pazienti possano ancora essere sfruttati per frodi o altre operazioni criminali*”, tra cui la condivisione in rete dei dati.

https://www.key4biz.it/sanita-irlandese-sotto-cyber-attacco-sconvolto-il-sistema-delle-prenotazioni-il-premier-martin-atto-atroce/361444/

Copasir, si dimette il presidente Volpi. Salvini: “Ora nuovo Comitato per sicurezza della Repubblica”

Il **Copasir** continua a “perdere pezzi”, a cominciare dal suo presidente **Raffaele Volpi** (Lega). Le sue dimissioni, insieme a quelle del senatore **Paolo Arrigoni**, sono state annunciate da **Matteo Salvini** in tarda mattinata, dopo l’abbandono dei lavori da parte dei componenti **M5S** e **PD**.

“Il presidente Raffaele Volpi e il senatore Paolo Arrigoni hanno lasciato l’incarico nel Copasir. Ora attendiamo le dimissioni di tutti gli altri componenti e la nomina di un altro comitato”, ha detto il leader della Lega

Inizia da ora il toto-nomine per il **Comitato parlamentare per la sicurezza della Repubblica**, che gestisce i dossier relativi alla sicurezza della Nazione.

M5s-Pd abbandonano lavori: “Trovare soluzione sulla presidenza”

Prima delle dimissioni dei leghisti Volpi e Arrigoni, oggi hanno abbandonato i lavori del Copasir anche **Federica Dieni**, **Maurizio Cattoi** e **Francesco Castiello** del **M5s** ed **Enrico Borghi** del **Pd**.

“Nel pieno rispetto delle prerogative istituzionali abbiamo votato la delibera adottata dall’ufficio di presidenza in ordine all’attivazione di quanto stabilito dall’art. 34 della legge 124/2007. Al tempo stesso, al fine di porre il Comitato al di fuori delle ripercussioni politiche e ripristinare quanto stabilito dal comma 3 dell’articolo 30, acquisita sul merito anche la condivisione del gruppo parlamentare di Leu, abbiamo abbandonato i lavori del Copasir al fine di contribuire alla soluzione della titolarità della Presidenza del comitato medesimo”. Così i componenti del Copasir Dieni, Cattoi, Castiello del M5s, e Borghi del Pd.

Copasir a mezzo servizio

Dopo lo strappo di **Adolfo Urso** di FdI ed **Elio Vito** di Fi, il Copasir non può contare sul numero completo dei suoi componenti. Lavora a mezzo servizio il **Comitato parlamentare per la sicurezza della Repubblica**. È grave.

Copasir, Fazzone: “Non mi dimetto, presidenti Camere risolvano questione della presidenza“

“Non mi dimetto e non entro nella diatriba sulla presidenza del Copasir. La questione non si risolve dimettendosi tutti ma con l’intervento di chi ha il ruolo, la funzione e la responsabilità di interpretare la legge, vale a dire i presidenti del Senato e della Camera”. L’ha detto all’Adnkronos il senatore del Gruppo Fi-Udc Claudio Fazzone, che respinge l’ipotesi di arrivare ad una nuova composizione del Copasir con metà rappresentanti della maggioranza e metà dell’opposizione, perché “*la legge parla di proporzionalità*”, ha concluso.

Risolvere la questione presidenza per lavorare sui dossier della sicurezza nazionale

La polemica sulla presidenza del Copasir deve essere risolta per il buon funzionamento del Comitato, perché la situazione che si è venuta a creare non aiuta al clima di collaborazione che ci deve essere tra componenti per lavorare sui dossier più delicati sulla sicurezza nazionale dell’Italia.

Copasir, cosa dice la legge di riferimento sulla presidenza

La legge di riferimento, la 124 del 2007, non è così esplicita, perché nel testo non c’è una espressa previsione di modifica dell’assegnazione della presidenza nel corso di una stessa legislatura, anche se cambia il Governo. Dunque, la legge è da modificare, semmai, per il futuro.

Ora per risolvere il problema attuale sulla presidenza del leghista Volpi, da sostituire, come da prassi con un esponente dell'opposizione (**FdI**), i presidenti di Camera e Senato sostengono sia necessaria una decisione da prendere a livello politico. Speriamo in tempi brevi.

https://www.key4biz.it/il-copasir-continua-a-perdere-pezzi-si-lavora-a-mezzo-servizio-sui-dossier-della-sicurezza-nazionale/361272/

Attacco Ransomware contro Axa Asia. Rubati 3 terabyte di dati sensibili

Una vera e propria vendetta. Le filiali del colosso assicurativo **AXA** con sede in Thailandia, Malesia, Hong Kong e Filippine sono state colpite da un ransomware.

Secondo quanto riporta **BleepingComputer**, il gruppo di criminal hacker **Avaddon** ha affermato sul proprio sito di di aver rubato 3 TB di dati sensibili dalle operazioni asiatiche del colosso assicurativo.

I dati compromessi ottenuti da Avaddon, secondo il gruppo, includono referti medici dei clienti, carte d'identità, estratti conto bancari, moduli di richiesta, registrazioni di pagamento, contratti e altro. Inoltre, il gruppo ha affermato che i siti Web di AXA con sede in Thailandia, Malesia, Hong Kong e Filippine erano soggetti ad un attacco DDoS.

Axa: addio alle polizze contro i ransomware

Appena una settimana fa il gruppo aveva annunciato l'esclusione dei danni correlati dalle proprie coperture assicurative da parte dei ransomware, una decisione presa a seguito delle preoccupazioni del Governo francese sugli enormi pagamenti che vanno ai criminali informatici a seguito delle polizze assicurative cyber di AXA e di altri assicuratori.

Il settore è stato recentemente oggetto di notevoli critiche per il rimborso dei pagamenti del riscatto. Con le polizze assicurative le organizzazioni sono più propense a pagare perché sanno che saranno rimborsate dal loro assicuratore. Ciò a sua volta ha portato a un aumento degli attacchi ransomware poiché i criminali informatici si sono resi conto che le aziende hanno maggiori probabilità di soddisfare le loro richieste.

Ranwomare: terzo incidente dopo Colonial Pipeline e il servizio sanitario irlandese

Al momento AXA, pur confermando l'avvenuto attacco, non ha fatto sapere se sia stato richiesto un riscatto o come la vicenda possa essere correlata agli annunci dei giorni scorsi.

"Asia Assistance è stata recentemente vittima di un attacco ransomware mirato che ha avuto un impatto sulle sue operazioni IT in Thailandia, Malesia, Hong Kong e Filippine. Una task force dedicata con esperti forensi esterni sta indagando sull'incidente. Le autorità di regolamentazione e i partner commerciali sono stati informati", ha dichiarato a BleepingComputer un portavoce di AXA.

"AXA prende molto sul serio la privacy dei dati e se le

indagini di IPA confermano che i dati sensibili di qualsiasi individuo sono stati interessati, verranno prese le misure necessarie per informare e supportare tutti i clienti aziendali e le persone interessate".

La tempistica intorno all'incidente è degna di nota considerando, questa settimana, il Federal Bureau of Investigation (FBI) e l'Australian Cyber Security Center (ACSC) avevano avvertito di attacchi ransomware Avaddon in corso contro organizzazioni di una vasta gamma di settori negli Stati Uniti e nel mondo.

Recentemente, il gruppo criminale informatico **DarkSide** ha chiesto 5 milioni di dollari per ripristinare le operazioni dell'oleodotto americano Colonial Pipeline.

E, proprio questa settimana, BleepingComputer ha riferito che i servizi sanitari irlandesi hanno raggiunto una richiesta di riscatto di 20 milioni di dollari.

https://www.key4biz.it/attacco-ransomware-contro-axa-asia-rubati-3-terabyte-di-dati-sensibili/360770/

Agenzia nazionale cyber, Mulè: "Sarà una struttura coordinata tra pubblico e privato"

"Con la nascita dell'Agenzia nazionale per la cybersecurity

*voluta dal prefetto **Franco Gabrielli** si sposterà l'asse della difesa cyber dal fronte dell'intelligence a un ambito residente all'interno della Presidenza del Consiglio, così da obbedire a un'esigenza già seguita da altri Paesi europei ed extraeuropei".*

Con queste parole il Sottosegretario alla Difesa **Giorgio Mulè**, intervenuto al webinar del Parlamento europeo in Italia su ***'La nuova strategia europea per rafforzare la sicurezza informatica'***, ritorna sull'idea del sottosegretario alla Presidenza del Consiglio **Franco Gabrielli**, di creare un'agenzia per cybersecurity non legata più al DIS. Gabrielli annunciò la nascita dell'Agenzia in questa intervista rilasciata in esclusiva di **Cybersecurity Italia,** a margine del convegno "*Le nuove reti per l'industria italiana e per i consumatori*" organizzato a Roma l'8 aprile 2021.

Mulè: "L'agenzia dovrà poggiare le fondamenta con una norma di primo livello"

"*L'agenzia*, ha aggiunto **Mulè** durante il webinar*, "dovrà nel più breve tempo poggiare le fondamenta nel tessuto legislativo con una norma di primo livello che vedrà il Parlamento coinvolto per recepirne gli indirizzi e le correzioni. L'obiettivo che si vuole raggiungere con l'istituzione dell'agenzia è quello di adeguare nel più breve tempo possibile il settore della cybersecurity alle mutate e sempre nuove esigenze nazionali e soprattutto internazionali con il superamento di un approccio che fino a questo momento privilegiava il fronte dell'intelligence al quale va dato atto e va detto che in un recente periodo storico ha supplito a carenze organizzative e strutturali che hanno contraddistinto il mondo della difesa cibernetica*".

“Ora e adesso, hic et nunc, si sente invece forte e non rinviabile l’esigenza di intraprendere in maniera decisa e coesa un’operazione di attualizzazione e di adeguamento del nostro comparto Cyber. La creazione di questa Agenzia per la cybersicurezza nazionale si pone proprio l’obiettivo di creare una struttura “votata” alla sicurezza cibernetica, in un’ottica di resilienza dell’infrastruttura digitale nazionale, assicurando il coordinamento tra i soggetti pubblici e privati coinvolti in tale materia”, ha continuato Mulè.

L’agenzia nazionale coniugherà il mondo civile con quello militare e di intelligence

“C’è l’esigenza di una sovranità nazionale tecnologica del Paese. La sfida dell’agenzia nazionale per la cybersecurity sarà quella di aprirsi e coinvolgere il mondo civile coniugandolo con quello militare e di intelligence. Attraverso questa interazione, il nuovo organismo potrà agire in maniera virtuosa creando una nuova cultura digitale che non dovrà limitarsi all’how to do riservata agli esperti, – ha aggiunto Mulè *– ma a quella di una formazione il più possibile ‘democratica’ non solo e non soltanto indirizzata agli addetti ai lavori ma che diventi sempre più cultura diffusa anche tra la popolazione civile”.*

“La cultura digitale è la sfida che, fin dal sistema scolastico, il Paese dovrà e deve affrontare subito. A questo proposito si sta lavorando al progetto per la creazione di una Cyber Defence Academy, cioè di un centro di alta formazione dove le esperienze maturate nel comparto difesa dovranno coniugarsi con le competenze già presenti nella pubblica amministrazione marciando in maniera osmotica con le imprese private”, ha concluso Mulè.

https://www.key4biz.it/agenzia-nazionale-cyber-mule-sara-una-struttura-coordinata-tra-pubblico-e-privato/360522/

Roberto Viola (DG Connect): “I centri nazionali della cybersecurity saranno finanziati con 1 miliardo di euro”

“Finanzieremo per circa 1 miliardo di euro i Centri operativi nazionali della cybersecurity a cui andranno le migliori tecnologie come l’Intelligenza Artificiale, i Big Data, e le migliori tecnologie per prevenire a gestire e migliorare l’ecosistema” della cybersecurity europea”. A dirlo è stato il Direttore Generale Dg Connect della Commissione europea, **Roberto Viola**, intervenendo alla conferenza **“La nuova strategia europea per rafforzare la sicurezza informatica”** nel corso della quale si sta discutendo il quadro finanziario 2021-2027 e i fondi Next Generation Eu per un piano d’investimento e innovazione che punti sulla cybersecurity.

“Come elemento della Strategia europea” per la cybersecurity, l’Unione europea ha adesso *“un Centro europeo per la sicurezza, sarà basato a **Bucarest** ma non sarà una cattedrale nel deserto perché sarà collegato a tutta una serie di Centri nazionali che lavoreranno insieme ed il regolamento prevede che tutti i centri nazionali lavoreranno insieme. Spero che*

l'Italia notifichi il centro di sicurezza nazionale al più presto, per poter iniziare ad usufruire del finanziamento. Avranno a disposizione le tecnologie migliori".

"Inoltre, ha sottolineato Viola, *"Ci saranno sanzioni per le aziende a fronte di negligenze delle industrie sulla cybersecurity che dovranno mettere in capo all'ad il tema della cybersecurity. Non è una minaccia ma una responsabilità, vogliamo una comunità che si assuma i rischi".*

Roberto Viola propone una ammodernamento delle infrastrutture per la cybersecurity

"Con la pandemia", ha spiegato il direttore Generale, *"abbiamo compreso che certe cose non accadono solo nei film di fantascienza ma accadono nella realtà e il rischio della cybersecurity è un rischio concreto con il quale dobbiamo fare i conti anche nel futuro*". Viola ha quindi evidenziato che *"le grandi Transizioni green e digitale hanno una vulnerabilità" per la grande mole di dati che attivano e per questo "sono esposte ad attacchi informatici". "Per questo* – ha ricordato Viola- *l'Ue ha messo in campo una strategia che si declina su 3 punti strategici fra cui un ruolo politico e più importante dell'Ue nel mondo" nella difesa dagli attacchi informatici*".

Viola ha citato fra le proposte di punta dell'Ue ai Paesi membri "proponiamo un ammodernamento" delle infrastrutture per la cybersecurity *"identificando i settori critici come la distribuzione dell'acqua, la distribuzione dell'energia, dei carburanti, delle aziende ospedaliere" tutti settori che "devono essere protetti e se c'è un incidente deve essere noto alle autorità perché così possano agire tutte insieme" come già avviene "per gli incidenti aerei". L'Ue, ha sottolineato ancora Viola, vuole anche "che il vertice di una società abbia*

la cybersecurity in capo al suo ad" ed "altro elemento della nuova direttiva vogliamo che ci sia una comunità che conosca i rischi informatici".

https://www.key4biz.it/roberto-viola-dg-connect-i-centri-nazionali-della-cybersecurity-saranno-finanziati-con-1-miliardo-di-euro/360487/

Sistema sanitario irlandese disattiva il sistema informatico: in corso attacco ransomware

Corrono ai ripari le autorità di Dublino, disattivando il sistema informatico dell'interno **Sistema sanitario nazionale**, l'*Health Service Executive* (Hse), a causa di un **attacco ransomware** definito "*di vaste proporzioni*".

I sistemi IT sono stati messi in standby per "*motivi precauzionali*", hanno commentato dall'Hse, soprattutto quelli relativi alle prenotazioni ospedaliere, con l'obiettivo di **mettere al riparo i dati sensibili dei pazienti e gli stessi sistemi operativi IT** delle strutture ospedaliere e sanitarie.

L'attacco informatico al sistema

sanitario irlandese

> *There is a significant ransomware attack on the HSE IT systems. We have taken the precaution of shutting down all our our IT systems in order to protect them from this attack and to allow us fully assess the situation with our own security partners.*
>
> *— HSE Ireland (@HSELive) May 14, 2021*

A livello mondiale il comparto sanitario e ospedaliero ha visto in quest'ultimo anno un incremento di attacchi informatici del +200% secondo stime NTT, a causa di un ricorso massiccio alla telemedicina e i servizi online soprattutto a causa della pandemia di Covid-19.

Come scritto dalla **BBC**, il Rotunda Hospital della capitale irlandese ha cancellato tutte le visite ambulatoriali, a meno di casi gravi e donne in gravidanza di oltre 36 settimane.

Interrotti anche i servizi del National Maternity Hospital di Holles Street sempre a Dublino.

Situazione grave secondo il CEO dell'Hse

L'amministratore delegato dell'Hse, **Paul Reid**, ha dichiarato al *Morning Irland* di RTE che l'attacco è "*significativo, di vaste proporzioni e considerato di livello grave*" e che presumibilmente è un ransomware.

Le conseguenze al momento non sono ancora note nella loro intera portata, ma già arrivano notizie di problemi su tutto il sistema sanitario nazionale e relativi all'offerta dei servizi primari.

Reid ha informato che l'attacco si sta concentrando

sull’accesso ai dati conservati nei server centrali e che non è arrivata nessuna richiesta di riscatto al momento.

“*Stiamo lavorando con tutti i nostri principali fornitori di sistemi di sicurezza IT. Lo stesso team informatico per la sicurezza nazionale è stato allertato ed è coinvolto nelle operazioni*”, ha dichiarato l’ad dell’Hse.

La preoccupazione di medici e pazienti

Il professor **Seamus O’Reilly**, oncologo del Cork University Hospital, ha raccontato a RTE che tutti i suoi computer sono stati spenti a causa dell’attacco informatico in corso, dicendosi preoccupato e “*angosciato*” per i pazienti in attesa dei risultati delle analisi, “*che ora vivono un una zona di incertezza*”.

Cresce quindi il disagio e la tensione, non solo tra il personale medico, ma anche tra gli stessi pazienti, alcuni dei quali soffrono di diverse patologie molto pesanti, come nel caso dei trattamenti anti-tumorali, che dipendono sempre più dalle nuove tecnologie, in questo momento ferme.

Krysia Lynch, presidente dell’Associazione per il miglioramento dei servizi di maternità in Irlanda, ha affermato che è giunto il momento di chiedere all’HSEs se i dati dei pazienti sono archiviati in modo sicuro e se dispongono di difese informatiche adeguate per gli attacchi ransomware.

https://www.key4biz.it/attacco-ransomware-al-sistema-sanitario-irlandese-e-vasto/360476/

Biden, nuovo provvedimento per rafforzare la cybersecurity USA. Intanto La Colonial Pipeline cede e paga il cyber riscatto

Firmato un **nuovo ordine esecutivo** dal Presidente degli Stati Uniti, **Joe Biden**, per potenziare i livelli di **cybersecurity** nel Paese dopo l'attacco ransomware agli oleodotti della **Colonial Pipeline** di questi giorni potato dal gruppo **DarkSide**.

> *The Colonial Pipeline incident is a sobering reminder that our nation faces sophisticated cyber threats.*
>
> *Today, President Biden signed an executive order to chart a new course to improve the nation's cybersecurity and protect federal government networks.* *https://t.co/j9wyCKdwj0 pic.twitter.com/bJxVYf2D72*
>
> *— The White House (@WhiteHouse)* *May 13, 2021*

L'executive order per riorganizzare le cyber difese nazionali

Un provvedimento necessario alla luce di quanta sta accadendo nel Paese e dei numerosi attacchi informatici che negli ultimi anni hanno preso di mira imprese, enti privati, gran parte della rete di agenzie federali e gli stessi dipartimenti del Governo americano.

Un atto dovuto e allo stesso tempo tardivo, che ha come obiettivo il contrasto forte alle moderne campagne informatiche sempre più dannose, persistenti e altamente sofisticate, in grado di infliggere gravi danni sia finanziari, sia materiali.

Così, mentre gli Stati Uniti ancora fanno i conti con una parziale scarsità di benzina, proprio per l'attacco del gruppo di cyber criminali DarkSide alle reti della Colonial Pipeline, Biden mette nero su bianco alcune misure volte a potenziare le difese cibernetiche nazionali.

La strategia di Biden

Prima di tutto, si legge nel documento ufficiale pubblicato dalla Casa Bianca, serve una maggiore circolazione di informazioni e di dati tra le agenzie governative e gli enti federali preposti alla difesa informatica, a cui devono contribuire anche le imprese fornitici di servizi IT.

Ogni informazione relativa a possibili vulnerabilità e attacchi informatici va condivisa tra enti pubblici e privati quindi e si dovrà poi creare un registro degli attacchi e delle risorse a disposizione per il contrasto degli stessi, gestito dal ***Cyber Safety Review Board***, con il fine ultimo di proteggere tutte le infrastrutture critiche e i servizi essenziali.

Colonial Pipeline intanto paga il riscatto a DarkSide

Il provvedimento è stato firmato poche ore dopo che la Colonial Pipeline ha annunciato il ripristino parziale delle attività di fornitura di carburante, ammettendo che comunque ci vorranno giorni prima di tornare agli standard operativi precedenti.

Secondo quanto pubblicato da *Bloomberg* ieri, per il riavvio delle infrastrutture e dei servizi l'utility avrebbe pagato un riscatto di 5 milioni di dollari in criptovaluta ai cyber criminali, nonostante abbia sempre dichiarato che non avrebbe versato un dollaro ai criminali informatici (come peraltro fortemente consigliato dall'FBI).

https://www.key4biz.it/biden-nuovo-provvedimento-per-rafforzare-la-cybersecurity-usa-intanto-la-colonial-pipeline-cede-e-paga-il-cyber-riscatto/360460/

Toshiba alle prese con un attacco ransomware in Europa. Ancora DarkSide

La filiale francese di **Toshiba** ha denunciato un attacco informatico stamattina e i colpevoli sembrano essere sempre i membri di **DarkSide**, il gruppo di cyber criminali che nei giorni scorsi ha mandato in tilt l'oleodotto della Colonial Pipeline negli Stati Uniti.

La notizia è stata pubblicata dalla Reuters e anticipata ieri dalla Japanese Broadcasting Association (NHK). Al momento "*solo una minima quantità di dati di lavoro pare possa esser andata persa*".

Si parla di un attacco di tipo **ransomware**, il che implica generalmente il sequestro di dati e/o intere infrastrutture e la richiesta di un riscatto in denaro molto corposo

solitamente.

Attacco ransomware

I cyber criminali di DarkSide sfruttano soluzioni "***Ransomware-as-a-Service***", che funziona come una catena di montaggio: un gruppo sviluppa il ransomware, gli affiliati eseguono l'attacco finale. Agli sviluppatori va circa il 20-30% del riscatto pagato dalla vittima.

Il gruppo in questione, sempre nella serata di ieri, ha pubblicato su Twitter un post in cui annunciava di esser entrata in possesso di **740 GB di dati sensibili**, relativi al personale, al management e alle attività operative.

> *[ALERT] DarkSide ransomware gang claimed to have leaked Toshiba France's sensitive data to the Darkweb. pic.twitter.com/JYjRDE4Chd*
>
> *— DarkTracer : DarkWeb Criminal Intelligence (@darktracer_int) May 13, 2021*

Toshiba in cattive acque

Il colosso giapponese non naviga in buone acque negli ultimi mesi. Complice la pandemia di Covid-19, la società sta ancora valutando l'offerta presentata ad inizio aprile del fondo di investimenti britannico CVC Capital Partners da 20 miliardi di dollari.

Una proposta che ha spaccato il board e determinato molto probabilmente le dimissioni del CEO di Toshiba, **Satoshi Tsunakawa**.

In questi giorni, la società giapponese stava valutando l'istituzione di un comitato revisore per stabilire una strategia finanziaria finalizzata ad aumentare il valore

dell’azienda e per questo motivo aveva nominato un team di consulenti provenienti dagli uffici svizzeri del **Gruppo UBS**.

Nel 2017 la Toshiba è stata già vittima di un attacco ransomware che prese di mira la produzione di memorie Nand Flash direttamente in Giappone. Gli impianti furono fermati per alcuni giorni, per concentrarsi sul contrasto al ransomware, causando enormi ritardi nell’approvvigionamento dei mercati e conseguenti danni economici.

https://www.key4biz.it/toshiba-alle-prese-con-un-attacco-ransomware-in-europa-ancora-darkside/360443/