Attacco ransomware Regione Lazio, Butti (FdI): “Il ministro Colao riferisca in aula”

“La Regione Lazio non è stata hackerata, è stata sbertucciata”. Lo ha riferito in aula alla Camera il deputato **Alessio Butti** di FdI a proposito dell’attacco ransomware subito dalla Regione Lazio lo scorso 1 agosto, chiedendo che il ministro Colao riferisca in Aula.

“C’e’ stato un durissimo colpo al sistema Cup della Regione – spiega Butti – *Sono saltate le visite specialistiche programmate, gli screening diagnostici, le prenotazioni dei vaccini e non era stato fatto backup dei dati. Chiediamo* – prosegue – *l’intervento del Generale Figliuolo per un’ordinata profilassi dei vaccini e al ministro di Colao che riferisca in Aula sui bandi di gara per i cloud della Pubblica amministrazione. Perché* – conclude Butti – *non vorremmo che” l’emergenza “portasse a procedure accelerate o facilitate”.*

L’attacco ransomware ha mandato in crisi anche la campagna vaccinale

Il sistema informatico della Regione Lazio è stato vittima di un attacco ransomware perpetrato la notte di domenica 1 agosto. Ancora oggi i sistemi sono fuori uso. L’attacco è andato a colpire il Centro elaborazione dati (CED), il sistema informatico che gestisce l’intera struttura informatica regionale, compresi i sistemi informatici che consentono di portare avanti la campagna regionale di vaccinazione per il

contrasto alla pandemia di Covid-19.

Il **CED** Lazio gestisce i dati sanitari e personali di quasi 6 milioni di cittadini. L'assessore alla Sanità del Lazio, **Alessandro D'Amato**, ha fatto sapere che al momento non c'è stata nessuna interruzione della campagna vaccinale, anche se in realtà di rallentamenti ce ne sono stati molti per le prenotazioni e non solo, ma è assicurata comunque la somministrazione dei vaccini.

Di fatto, anche in Italia, gli attacchi informatici sono in aumento e questo in particolare ha dimostrato di potere mettere in difficoltà seria la fornitura di un servizio essenziale per la comunità, come quello pubblico sanitario.

L'amministrazione pubblica tra i settori più colpiti dai cibercriminali

Secondo i dati dello studio condotto dall'americana SonicWall, solo nel mese di giugno 2021 sono stati registrati in tutto il mondo più di 78 milioni di attacchi ransomware. Da gennaio a oggi sono stati misurati due picchi notevoli: +185% negli Stati Uniti e +144% nel Regno Unito.

I settori più colpiti sono stati quello dell'amministrazione pubblica, quindi il Governo centrale e locale, con un aumento allarmante del +917% in un solo anno, seguito dall'istruzione (+615%), la sanità (+594%) e la vendita al dettaglio o retail (+264%).

Combattere i ransomware una volta che hanno preso possesso di un apparecchio o un sistema informatico è difficile, molto più facile ed efficace risulta prevenirli, magari con backup continui dei dati (altro obiettivo primario dei cibercriminali).

l ransomware sono pericolose e potenti entità malevole ibride, capaci non solo semplicemente di cifrare dati e chiedere un riscatto (in inglese ransom significa proprio riscatto), ma anche di diffondersi massivamente in rete, interrompere la continuità operativa e causare gravi fughe di dati sensibili, diventando, di fatto, una delle più grandi minacce alla sicurezza del cyber spazio.

La diffusione dei dispositivi dell'Internet delle cose, dei servizi cloud e della digitalizzazione ha inoltre accresciuto il grosso potenziale di pericolosità dei malware del riscatto, portandoli a influenzare non solo la nostra vita quotidiana, minando la sicurezza dei nostri dispostivi ma anche a compromettere servizi e intere reti aziendali.

https://www.key4biz.it/attacco-ransomware-regione-lazio-butti-fdi-il-ministro-colao-riferisca-in-aula/371078/

Zingaretti. Perché quelle inutili bugie sull'attacco informatico alla Regione Lazio?

A quasi 72 ore dall'attacco informatico ai sistemi informativi della **Regione Lazio**, permangono ancora le iperboli usate dal presidente della Regione **Nicola Zingaretti**, che continua a ripetere la sua versione. Una versione nella quale insiste per la verità solo lui, dal momento che nessun altro soggetto

istituzionale o amministrativo (polizia giudiziaria o magistratura) ha proferito parola sull'accaduto.

"Attacco terroristico"? Ma in base a quali evidenze?

Zingaretti ci ha tempestivamente e inequivocabilmente informato tutti della matrice terroristica dell'attacco. In base a quali evidenze? Nessuna delle istituzioni preposte alla vigilanza e alla difesa da atti di terrorismo ha detto alcunché, ma lui ha ripetuto per due giorni la sua versione. Nessuno sa da dove Zingaretti abbia ricavato questa informazione. Se Zingaretti avesse ragione sarebbe un fatto di enorme gravità che metterebbe a repentaglio l'intera comunità nazionale. Ma Zingaretti non ci dice nulla sulla fonte delle sue informazioni e insiste nello spargere terrore su matrici che potrebbero inevitabilmente essere di vario tipo. Fondamentalismo arabo? Nuclei armati esteri? Gruppi nazionalistici armati di altri Paesi? Ce lo dica….

"Attacco proveniente dalla Germania"? Ma perché non dal vicino di casa?

Zingaretti ci dice che l'attacco proviene "…*da un Paese estero*…", anzi dalla Germania. Ma chi lo ha appurato e come si fa ad appurare con certezza la provenienza geo-referenziata di un attacco in cosi poco tempo e in modo affidabile? Dettagli che sfuggono a Zingaretti che spara la sua teoria senza alcuna pezza d'appoggio. In questi casi gli esperti lavorano a volte settimane, se non mesi, per appurare in dettaglio la fonte esatta dell'attacco. Ma per Zingaretti è un gioco da ragazzi. Lui evidentemente sa già.

“Il più grande attacco mai registrato in Italia”? Ma neanche per sogno

Zingaretti ci informa anche che si è trattato del più grande attacco *ransomware* mai fatto in Italia, anzi “*…mai subito dalle istituzioni repubblicane*”. Anche se Zingaretti stesso si affretta a dire paradossalmente che sono stati sottratti pochi dati e non è stato chiesto alcun riscatto…

Ma in base a quali analisi definisce quello della Regione Lazio come il più grave attacco informatico? Non si sa, anzi verrebbe voglia di chiedergli chi gli suggerisca queste uscite ad effetto. L’Italia ha registrato tanti grandi attacchi negli ultimi anni e quello della Regione Lazio al momento ha le dimensioni di un caso ordinario. In molti ricorderete l’attacco continuativo, perché non scoperto se non dopo molti mesi, ai danni del ministero degli Affari Esteri, che trafugò documenti diplomatici a beneficio di potenze straniere, giusto per citarne uno dei tanti.

Come si vede, si tratta di tre uscite infelici del Presidente della Regione Lazio, che non hanno una spiegazione convincente, mentre nessun altro soggetto istituzionale o amministrativo ha proferito parola in questi due giorni e la consegna sembra essere quella della prudenza e della cautela.

Nessun elemento emerge peraltro neanche dalla primaria società di informatica fornitrice della Regione Lazio, anche se sembra che nei giorni precedenti qualcuno avesse allertato sulla possibilità di una condizione di emergenza informatica e di un possibile attacco.

Tutto questo pandemonio avviene esattamente nei giorni in cui si sta convertendo in legge l’atto che istituisce l’**Agenzia Nazionale di Cybersicurezza**, un atto importante per mettere in maggior sicurezza il Paese e i suoi dati.

Non vorremmo, tuttavia, che il clima di ingiustificata paura intorno a un caso del tutto ordinario di sicurezza informatica, come quello della Regione Lazio, scatenata dal Governatore serva a legittimare procedure in deroga rispetto ai piani ordinari di bandi di gara per il **Cloud** della **Pubblica Amministrazione**.

Non c'è alcuna emergenza e le procedure del **Cloud nazionale** devono procedere come previsto, per assicurare allo Stato il controllo dei dati dei cittadini.

Il ministro **Vittorio Colao** segue le prassi ordinarie per assicurare al Paese le scelte migliori e quelle più ponderate in ambito di **Cloud**.

Questi dati prima o poi andranno sul **Cloud** e vogliamo che sia un **Cloud** sicuro, saldamente sotto il controllo dello Stato e che coinvolga le imprese italiane, ma tutto secondo le procedure ordinarie.

https://www.key4biz.it/zingaretti-perche-quelle-inutili-bugie-sullattacco-informatico-alla-regione-lazio/371025/

Data breach, in Italia nel 2020 danni per 3,03 milioni di euro. Lo studio di IBM security

I data breach costano alle aziende 4,24 milioni di dollari in media per ogni incidente: questa la principale evidenza dell'ultimo ***"Cost of a Data Breach Report",*** lo studio condotto

da **Ponemon Institute** e promosso da **IBM Security**.

L’escalation della violazione dei dati, spiega IBM, è dovuto in gran parte ai rapidi mutamenti dettati dalla pandemia, come la riorganizzazione del lavoro da remoto e la rapida migrazione dei business verso un approccio “cloud-based” per garantire continuità delle attività.

Data breach: in Italia costo delle violazioni è salito a 3,03 milioni di euro

Nel 2020 in Italia, spiega l’indagine di IBM Security, il

costo complessivo delle violazioni di dati è salito a 3,03 milioni di euro e il costo per ogni informazione rubata a 135 euro, valore quasi raddoppiato nell'ultimo decennio.

I settori più colpiti da attacchi informatici sono stati i servizi finanziari (171 euro per informazione rubata), il settore energetico (165 euro) e quello farmaceutico (164 euro). I giorni per identificare e contenere una minaccia informatica, spiega lo studio, sfiorano ancora la soglia dei 250, anche se il trend è in leggera discesa.

La pandemia da COVID-19 ha messo in luce le evidenti difficoltà delle aziende in ritardo nella trasformazione digitale. Le aziende che non hanno nemmeno cominciato il processo di digitalizzazione o lo hanno incominciato da poco (magari in seguito alla pandemia), sono le più esposte ad attacchi informatici e quelle che ne pagano le conseguenze, anche economiche, più care (3,75 milioni di euro vs. 2,72 milioni di euro rispetto a chi è già in una fase matura del processo).

I trend a livello mondiale: dal remote working, alla sanità passando per le credenziali compromesse

Nel 2020, le aziende sono state costrette a modificare rapidamente il proprio approccio alla tecnologia, incoraggiando o obbligando i dipendenti a ricorrere al lavoro da remoto durante la pandemia e il 60% delle imprese si è spostato verso un approccio cloud-based per condurre le proprie attività. I dati pubblicati oggi evidenziano, però, che la security potrebbe non essersi adeguata altrettanto velocemente, ponendo un freno alla capacità delle organizzazioni di rispondere alle violazioni dei dati. La prima causa è da attribuire al rapido passaggio delle attività

lavorative verso lo smart-working sembrerebbe aver causato data breach più costosi: oltre 1 milione di dollari in più in media quando il lavoro remoto è stato indicato come causa dell'evento dalle aziende analizzate, rispetto alle violazioni con altri vettori (4,96 dollari contro 3,89 milioni di dollari per ogni violazione).

Per lo studio i settori che hanno affrontato enormi cambiamenti operativi durante la pandemia hanno anche sperimentato un crescente aumento della spesa per i data breach. Il settore sanitario è quello che paga il prezzo di gran lunga più caro, con 9,23 milioni di dollari per incidente – un aumento di 2 milioni di dollari rispetto all'anno precedente.

Le credenziali utente rubate sono state la causa principale delle violazioni. Allo stesso tempo, i dati personali degli utenti (come nome, e-mail, password) sono stati tra le informazioni più comunemente esposte, presenti nel 44% delle violazioni analizzate. La combinazione tra questi fattori potrebbe causare un effetto a spirale in futuro, con username e password rubate che diventano potenziali agganci per portare a termine ulteriori aggressioni.

L'impatto del lavoro a distanza e della migrazione al cloud sui data breach

Con l'aumento delle interazioni digitali portato dalla pandemia, le organizzazioni hanno adottato il lavoro da remoto e il cloud per soddisfare la crescente domanda di attività online. Lo studio ha rilevato che tali fattori hanno avuto un impatto significativo sulle violazioni di dati: quasi il 20% delle organizzazioni analizzate dallo studio ha riferito che lo smart working è stato un fattore chiave nelle violazioni dei dati e che le violazioni causate da smart-working sono

costate alle aziende 4,96 milioni di dollari, il 15% in più rispetto al costo medio.

Inoltre, le aziende intervistate che hanno subito una violazione durante un progetto di migrazione al cloud hanno affrontato un costo superiore del 18,8% rispetto alla media. Tuttavia, l'indagine ha anche rilevato che le organizzazioni più "mature" nella strategia di modernizzazione del cloud sono state in grado di identificare e rispondere più efficacemente agli incidenti, impiegando circa 77 giorni in meno rispetto alle imprese in fase iniziale di adozione. Infine, per le violazioni di dati avvenute sul cloud, le organizzazioni che hanno adottato un approccio hybrid cloud hanno dovuto affrontare una spesa più contenuta (3,61 milioni di dollari) rispetto alle imprese che avevano adottato un approccio principalmente di cloud pubblico (4,80 dollari) o privato (4,55 milioni di dollari).

Credenziali compromesse: un rischio crescente

Il rapporto ha anche fatto luce su un problema crescente: i dati dei consumatori, incluse le credenziali, compromessi durante un data breach possono poi diventare leva per propagare ulteriori attacchi. Se si considera che l'82% delle persone intervistate ammette di riutilizzare le password tra gli account, le credenziali compromesse sono sia la causa che l'effetto principale delle violazioni, un problema che rappresenta un rischio crescente per le aziende.

- **Dati personali esposti:** quasi la metà (44%) delle violazioni analizzate ha esposto i dati personali dei clienti, come nome, e-mail, password, o anche dati sanitari, rappresentando dunque il tipo più comune di informazione rubata.
- **Le informazioni personali costano di più:** la perdita di PII (Personal Identifiable Information) dei clienti è

stata anche il tipo di violazione più costosa (180 dollari per record perso o rubato contro 161 dollari di media).

- **Metodo di attacco più comune**: le credenziali utente compromesse sono state il metodo più comune utilizzato come punto d’ingresso dagli aggressori (20% delle violazioni studiate).
- **Più lunghi da rilevare e contenere:** le violazioni frutto di credenziali compromesse sono state quelle che hanno richiesto più tempo per essere rilevate, 250 giorni contro i 212 di media.

AI, security analytics e crittografia per mitigare gli attacchi

“L’aumento dei costi di data breach è un’altra spesa che si aggiunge a quelle che le aziende hanno dovuto affrontare, sulla scia dei rapidi cambiamenti causati dalla pandemia”, ha affermato Chris McCurdy, Vice President e General Manager, IBM Security. “*Tuttavia, sebbene i costi delle violazioni abbiano raggiunto un livello record nell’ultimo anno, lo studio ha anche mostrato segnali positivi rispetto all’adozione di tecnologie e approcci innovativi di cybersecurity, come l’AI, l’automation e l’approccio ‘Zero Trust’, che possono contribuire a ridurre il costo degli incidenti con ritorni anche per il futuro*.”

AI, security analytics e crittografia, per IBM security, sono stati i primi tre fattori di mitigazione delle violazioni, dimostrando come queste tecnologie possano ridurre i costi per singolo attacco. Le aziende che si sono dotate preventivamente di questi strumenti hanno risparmiato tra 1,25 e 1,49 milioni di dollari rispetto alle organizzazioni che non ne hanno fatto un uso significativo.

Per quanto riguarda i data breach basati sul cloud, le imprese con una strategia hybrid cloud hanno dovuto affrontare una spesa inferiore (3,61 milioni di dollari) rispetto alle organizzazioni che avevano adottato un approccio principalmente di cloud pubblico (4,80 milioni di dollari) o privato (4,55 milioni di dollari).

https://www.key4biz.it/data-breach-in-italia-nel-2020-danni-per-303-milioni-di-euro-lo-studio-di-ibm-security/370364/

Polizia di Stato, ecco come funziona il Cyber Security Operations Center (C-SOC) di Roma a tutela delle banche dati

Sovente, l’innovazione, nella sua accezione più ricca e variegata, tende la mano alla pubblica amministrazione. Non di rado, ma finora non quanto auspicato, l’amministrazione pubblica raccoglie il testimone dell’innovazione avvalendosi delle forme di finanziamento che, sempre più strutturate, arrivano dall’Unione Europea. Incessantemente, a esperienza di chi scrive, l’azione amministrativa è “trainata” dalla responsabilità di doversi conformare a leggi e regolamenti, sebbene con tempistiche di adeguamento non sempre proporzionate.

È allora edificante, in apertura di questo secondo semestre di un 2021 denso di buoni propositi e complesse opere di pianificazione e rilancio, narrare di una concreta e ben riuscita esperienza che ha saputo coniugare l’innovazione, gli stanziamenti dell’Unione Europea e il tempestivo adeguamento alla norma, nel progetto di realizzazione del **Cyber Security Operations Center** (nel seguito C-SOC) della **Direzione Centrale Polizia Criminale**, articolazione del Dipartimento della Pubblica Sicurezza del Ministero dell’Interno che, oltre a mantenere vive ed operative le relazioni internazionali nei

consessi di *law enforcement* (Europol, Interpol, etc.), ospita e gestisce le banche dati interforze (Centro Elaborazione Dati, Sistema Informativo Schengen Nazionale, Banca Dati Nazionale del DNA, Numero Unico di Emergenza 112).

Il C-SOC è stato inaugurato il 26 aprile alla presenza delle massime autorità e dei vertici delle amministrazioni operanti nell'ambito della pubblica sicurezza nazionale: Ministro dell'Interno – Autorità Nazionale di Pubblica Sicurezza, Sottosegretario di Stato – Autorità delegata alla sicurezza della Repubblica, Capo della Polizia – Direttore Generale della Pubblica Sicurezza, comandanti e direttori generali delle forze di Polizia nazionali.

Le presenze illustri non si sono esaurite con l'eccellente partecipazione dei vertici dell'intero comparto sicurezza ma hanno visto, quale ospite di pregio, il Segretario Generale dell'Autorità Garante per la protezione dei dati personali. La presenza del Garante Privacy attesta, anticipando ciò che si avrà modo di illustrare più avanti, la duplice natura del C-SOC: strumento a presidio della cyber security delle banche dati interforze e, al contempo, strumento a protezione delle persone fisiche i cui dati personali sono trattati per finalità di polizia.

Il C-SOC, il cui front-office operativo – sito inaugurale d'eccezione – è solo la parte visibile di un *iceberg* fatto di diritti fondamentali e significative competenze giuridiche, tecniche ed amministrative, consente, in estrema sintesi, di congiungere la protezione dei dati personali, la protezione dell'individuo e la protezione della collettività all'interno del cyber-spazio interforze…

Clicca qui per continuare a leggere l'articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/polizia-di-stato-ecco-come-funziona-il-

cyber-security-operations-center-c-soc-di-roma-a-tutela-delle-banche-dati/370053/

Spyware, in Israele task force sul caso Pegasus. Stefano Mele: 'Problema non sono le aziende'



Il governo di Israele ha creato una task force per gestire la crisi innescata dal caso **Pegasus**, lo spyware creato da un'azienda privata israeliana – la **NSO** – e venduto anche a regimi che l'hanno usato per operazioni illegali.

Secondo quanto riporta il Guardian, una squadra che comprende rappresentanti del ministero della Difesa, del ministero della

Giustizia, del ministero degli Esteri, dell'intelligence militare e del Mossad, l'agenzia di intelligence nazionale, è pronta a condurre un'indagine sulla necessità di "cambiamenti politici" per quanto riguarda le esportazioni informatiche sensibili.

Vendita Spyware Pegasus: le aziende sono autorizzate dai governi

La creazione della task force arriva in un momento in cui, la pressione diplomatica su Israele, aumenta di giorno in giorno. Le preoccupazioni hanno tutti un'unico comune denominatore. Pare che il governo abbia consentito licenze di esportazione per lo spyware a Paesi autoritari e repressivi.

La NSO ha venduto Pegasus ad altre nazioni grazie ad una licenza gestita dal governo israeliano, che può autorizzare oppure bloccare il contratto considerata la pericolosità del software. In questi anni Pegasus era diventato "il giocattolo che tutti volevano" – definizione di un esperto anonimo sentito dal Financial Times – e quindi era nata una "diplomazia Pegasus" che ruotava attorno alla concessione dello spyware. E questa diplomazia precedeva di molto le relazioni diplomatiche ufficiali.

Resta inoltre da chiarire se le agenzie di intelligence israeliane siano state in grado di accedere alle informazioni raccolte dai clienti della NSO, cosa che sia Israele che la società di sorveglianza negano fermamente.

Il ministro della Difesa, **Benny Gantz,** ha ammesso che Israele stava "studiando" le rivelazioni del progetto Pegasus su NSO appena emerse. *"Approviamo l'esportazione di prodotti informatici solo ai governi e solo per uso legale"*, ha affermato in un discorso a una conferenza informatica all'Università di Tel Aviv. *"I Paesi che acquistano questi software devono soddisfare i termini di utilizzo".*

I timori dei funzionari sembrano anche essere incentrati su come le rivelazioni del progetto Pegasus influenzeranno altre società israeliane e il futuro dell'industria informatica israeliana, considerata una delle migliori a livello mondiale…

Continua a leggere l'articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/spyware-in-israele-task-force-sul-caso-pegasus-stefano-mele-problema-non-sono-le-aziende/369649/

Spyware e intercettazioni: il precedente italiano con Exodus



In questi giorni si fa un gran parlare del grande attacco informatico portato a politici, giornalisti, professionisti e attivisti per i dritti umani in più Paesi nel mondo, attraverso lo spyware “**Pegasus**”, realizzato dalla società **NSO**.

Lo spyware, un software di livello militare, nato per per consentire ai governi di penetrare le reti di terroristi e criminali, sarebbe stato usato dall’Arabia Saudita per spiare i cellulari di alcune persone vicine a **Jamal Kashoggi,** giornalista ucciso nel consolato saudita a Istanbul nel 2018.

Lo scandalo è emerso grazie a un’indagine condotta per mesi dall’organizzazione giornalistica no profit francese **Forbidden Storie**s in collaborazione con Amnesty International. Alle ricerche hanno partecipato 16 media di vari Paesi, tra cui i quotidiani **“The Washington Post”, “Sueddeutsche Zeitung”, “Le Monde”** e **“The Guardian”.**

Spyware Pegasus: anche il presidente Macron coinvolto

Come riferito ieri da “Le Monde” anche un telefono cellulare del presidente francese, **Emmanuel Macron**, è stato spiato dal Marocco attraverso il software Pegasus.

Secondo le informazioni raccolte, nel marzo del 2019 un agenzia dell’intelligence marocchina ha utilizzato Pegasus per spiare uno dei numeri telefonici del capo dello Stato francese. Nel mirino di Rabat anche i telefoni dell’ex premier, Edouard Philippe, e di 14 altri ministri. L’Eliseo ha commentato al quotidiano “Le Monde” l’informazione, affermando che se dovesse essere confermata sarebbe molto “grave”. Nei giorni scorsi la Procura di Parigi ha aperto un’inchiesta dopo le denunce presentate da Edwy Plenel, direttore di Mediapart, e da Lenaig Bredoux, giornalista della stessa testata.

Continua a leggere l’articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/spyware-e-intercettazioni-il-precedente-italiano-con-exodus/369291/

Spyware, Snowden: “L’industria va fermata. Diffondono virus, non

vaccini”



Per **Edward Snowden,** l’informatico statunitense che ha rivelato al mondo lo scandalo dei programmi di sorveglianza di massa della NSA, “questa fuga di notizie sarà la storia dell’anno”. Ma a cosa si riferisce? Procediamo con ordine.

Decine di politici, attivisti e giornalisti in tutto il mondo sono stati spiati grazie ad un spyware installato nei loro cellulari. Si chiama **Pegasus** e lo ha sviluppato un’azienda israeliana, la **NSO**, che poi l’ha venduto a numerosi paesi, tra cui vari regimi autoritari. Tra gli acquirenti figura anche l’Ungheria di **Viktor Orban.**

La **NSO Group** è l’organizzazione di hacker su commissione più famigerata al mondo, e Pegasus è lo spyware di punta del gruppo. Il software di livello militare, nato per per consentire ai governi di penetrare le reti di terroristi e criminali, è un malware che infetta gli iPhone e gli smartphone Android per consentire a chi lo opera di accedere

ai dispositivi ed estrarre messaggi, foto, email e anche per attivare segretamente il microfono e la telecamera del dispositivo. NSO Group nega che i dati siano trapelati dai suoi server e definisce il rapporto di Forbidden Stories *"pieno di ipotesi errate e teorie non confermate".*

Snowden: "Presto gli obiettivi non saranno più 50mila ma 50 milioni"

Intervistato dal Guardian, una delle testate che ha realizzato lo scoop su Pegasus, il cyber attivista tuona contro la l'assenza di regolamentazione dell'intero settore. *"Se non si fa nulla per fermare la vendita di questi software, gli obiettivi non saranno più 50mila ma 50 milioni. E questo avverrà molto rapidamente"*, spiega al quotidiano inglese…

Continua a leggere l'articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/spyware-snowden-lindustria-va-fermata-diffondono-virus-non-vaccini/369136/

Cyberwar, gli Stati Uniti e i suoi alleati fanno fronte comune contro la Cina



Una nuova alleanza composta da Stati membri della NATO, Unione Europea, Regno Unito, Giappone e i paesi dell'ex Anzus Pact, Australia e Nuova Zelanda, fa fronte comune contro gli attacchi informatici sponsorizzati dalla Cina.

In una conferenza stampa tenutasi domenica 18 luglio, un alto funzionario della Casa Bianca ha preannunciato la dichiarazione congiunta degli Stati Uniti e dei suoi alleati contro la Repubblica popolare cinese per attività informatiche dannose e comportamenti irresponsabili. In particolare, la dichiarazione indica la Cina come una minaccia per l'economia e la sicurezza nazionale degli alleati.

Si tratta dunque di una dichiarazione di portata storica perché, per la prima volta, come sottolineato dal funzionario statunitense, la NATO condanna le attività cibernetiche della Repubblica popolare cinese. La guerra tecnologica e informatica riflette dunque la lotta di potere globale tra democrazie e stati autocratici. In questo contesto, la nuova alleanza per la sicurezza informatica potrebbe diventare un modello per affrontare le future minacce transnazionali.

Attacco a Microsoft Exchange Server: gli Usa accusano la Cina

La dichiarazione si concentra, in particolare, sull'attacco compiuto a danno dei server di posta elettronica di Microsoft Exchange all'inizio di quest'anno.

L'attacco è stato effettuato da hacker appartenenti a una rete di spionaggio soprannominata **Hafnium** alle dipendenze del ministero della Sicurezza di Stato cinese per svolgere attività criminali, come l'estorsione cibernetica, il crypto-jacking e il furto a vittime in tutto il mondo per guadagni economici. "In alcuni casi, siamo a conoscenza di rapporti che gli operatori cibernetici affiliati al governo della Repubblica Popolare Cinese hanno condotto operazioni di ransomware contro aziende private, che hanno incluso richieste di riscatto di milioni di dollari", ha affermato il funzionario.

Inoltre, l'FBI, la National Security Agency e la Cybersecurity and Infrastructure Security Agency hanno rilasciato un report che elenca 50 tattiche, tecniche e procedure impiegate dagli hacker sponsorizzati dallo stato cinese.

Nessuna sanzione

La formazione della coalizione anti cinese è l'ultima iniziativa dell'amministrazione Biden contro Pechino. Tuttavia, anche se "gli Stati Uniti e i loro alleati e partner non escludono ulteriori azioni…

Continua a leggere l'articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/cyberwar-gli-stati-uniti-e-i-suoi-alleati-fanno-fronte-comune-contro-la-cina/369097/

Cybercrime, ‘La soluzione contro gli attacchi ransomware? Sanzionare chi paga il riscatto’

Il crimine informatico continua a a far parlare di sé. Dopo l’ultimo eclatante colpo del ransomware **REvil** alla **Kaseya** il gruppo di criminal hacker ha alzato un polverone attirando l’attenzione di molti governi e rispettivi apparati di sicurezza. Da martedì la banda di REvil sembra scomparsa: siti web, infrastrutture e computer riconducibili a questi cybercriminali sono offline. I motivi sono ignoti ma le ipotesi sono sostanzialmente tre. Abbiamo fatto una chiaccherata con **Annita Sciacovelli**, prof.ssa di Diritto dell’Unione europea dell’Università degli studi di Bari ‘Aldo Moro’ & *cybersecurity specialist*, per capire lo stato dell’arte del crimine informatico.



Prof.ssa Annita Sciacovelli

Cybersecurity Italia. ***Prof.ssa Sciacovelli, REvil, il gruppo di hacker russi più grande e pericoloso al mondo è sparito dal web. Nessuno, al momento, conosce la genesi del black-out.***

Secondo lei cosa è successo? A chi dobbiamo attribuire la scomparsa del gruppo ransomware più ricco e famoso al mondo. Biden o Putin?

Annita Sciacovelli. Effettivamente, non è chiaro il motivo della scomparsa dal dark web di tutte le pagine e del portale di **REvil**. Escluderei un intervento di law enforcement delle autorità russe, che altrimenti sarebbe stato ampiamente pubblicizzato. Possiamo formulare qualche ipotesi, come la scelta della cyber gang di assumere un profilo basso o di apparire successivamente con un altro brand. Raramente, le cyber gang spariscono. Peraltro, all'indomani del duro colpo inferto alla **Colonial Pipeline**, anche il gruppo DarkSide si è dileguato. Un'altra ipotesi può riguardare una cyber retaliation del Governo americano, minacciata la settimana scorsa durante il confronto tra Putin e Biden che sembra essersi materializzata nel recentissimo attacco cyber al ministero della difesa russo. Infine, non possiamo escludere che Putin abbia chiesto a REvil di uscire di scena temporaneamente, il che giustificherebbe la matrice russa dell'attacco.

Cybersecurity Italia. ***Dopo i gravi attacchi informatici alle infrastrutture critiche, uno su tutti l'attacco al Colonial Pipeline, qual è l'approccio migliore per affrontare la minaccia ransomware?***

Annita Sciacovelli. L'approccio migliore si basa sul motto che la cybersecurity è troppo importante per considerarla appannaggio esclusivo degli …'addetti a lavori'! Bisogna sollecitare il mondo politico e l'opinione pubblica sulle gravi conseguenze derivanti dagli attacchi informatici che, se condotti su ampia scala, sono una minaccia alla pubblica sicurezza dello Stato, pericolosa anche per il comparto economico e sanitario (v. Estonia 2007, Ucraina 2017 e Georgia 2019).

Basti pensare che il ransomware di cui è stato vittima il

Sistema sanitario irlandese il mese scorso, che ha messo fuori uso i sistemi informatici di molti ospedali, ha avuto (e avrà) gravi conseguenze anche in termine di vite umane. Si stima che ci vorranno mesi prima che venga ripristinato il suo normale funzionamento, con un costo presunto che si aggira intorno ai 100 milioni di euro. Conviene imparare da questi episodi per investire in prevenzione cyber in ambito pubblico e privato. Sul punto, può essere utile ricordare che la Cyber Agency israeliana ha pubblicato una guida in cui, tra l'altro, consiglia la creazione di un team di gestione delle crisi, al quale spetta il compito organizzare regolarmente esercitazioni per affrontare attacchi cyber.

'La soluzione contro gli attacchi ransomware? Sanzionare chi paga il riscatto'

In realtà, dovremmo valutare l'ipotesi di sanzionare chi paga il riscatto: mi sembra una delle poche soluzioni per spezzare il circolo vizioso di un reato che favorisce lo sviluppo delle cyber gang, come di recente paventato dal Governo francese. Ricordiamo che per ogni singolo colpo a infrastrutture critiche il riscatto può ammontare anche a una decina di milioni di dollari. In proposito, non trascurerei il fatto che il pagamento del riscatto, da parte di enti pubblici o privati, può essere una condotta capace di integrare una serie di reati tra cui la creazione di una provvista di pagamento che potrebbe configurare il reato di false comunicazioni sociali, ovvero il reato di finanziamento della criminalità organizzata, oltre che la violazione di principi e valori dichiarati nel Codice etico e in materia di responsabilità sociale d'impresa.

Cybersecurity Italia. ***Dal suo punto di vista, quale approccio consiglia per combattere il crimine informatico?***

Annita Sciacovelli.In termini più generali, dalla mia attività di ricerca sulla cybersecurity emerge un duplice schema di risposta al crimine informatico, basato su un approccio che prevede, in primo luogo, l'impegno del legislatore statale a redigere un **testo unico di cyber diritto**. E' noto che il nostro ordinamento reca già una serie di disposizioni repressive in materia, si pensi proprio al contrasto al ransomware, sebbene per altri illeciti non è così perché ad essi sono inapplicabili le tradizionali categorie penali.

In secondo luogo, a livello internazionale è necessaria l'elaborazione di una disciplina sulla **attribution** che sia ritagliata a seconda delle diverse tipologie di reati e attacchi cyber in cui possono essere coinvolti, a vario titolo e modo, attori non statali e Stati. Infatti, il problema della repressione degli illeciti informatici non riguarda la loro criminalizzazione, sancita dalla Convenzione di Budapest sulla criminalità informatica del 2001 e firmata dall'Italia, bensì l'assenza di un protocollo internazionale sulla digital forensic e sulla cooperazione internazionale nell'attività investigativa digitali, atteso che si tratta di illeciti transnazionali.

In questo solco, si inserisce il **Joint Statement** firmato tra i 27 Paesi dell'UE e il Segretario americano della Homeland Security, **Alejandro Mayorkas**, a Lisbona il 22 giugno scorso, che prevede l'adozione di una strategia di contrasto al malware; la cooperazione anche in materia di *disclosure* e l'impegno degli Stati di attivarsi per arrestare, perseguire o estradare i presunti criminali che compiono reati informatici sul loro territorio, nel rispetto del principio di *due diligence*...

Continua a leggere l'articolo su Cybersecurity Italia su cui è stato originariamente pubblicato.

https://www.key4biz.it/cybercrime-la-soluzione-contro-gli-attacchi-ransomware-sanzionare-chi-paga-il-riscatto/368917/

Ransomware REvil, il gruppo criminal hacker più pericoloso al mondo è scomparso dal web



REvil, il gruppo di hacker russi più grande e pericoloso al mondo è sparito dal web. Nessuno, al momento, conosce la genesi del black-out.

Secondo quanto riporta il New York Times, il primo a dare la notizia, il merito della scomparsa del gruppo di cybercriminali è da attribuire a **Joe Biden** e **Vladimir Putin**.

Il presidente degli Stati Uniti, lo scorso 9 luglio, aveva dichiarato di aver parlato al telefono con il presidente russo

proprio per sollevare la questione relativa agli attacchi informatici che nei mesi scorsi sono sembrati provenire dalla Russia, e che già erano stati oggetti di discussione durante l'incontro a Ginevra dello scorso 16 giugno tra USA e Russia.

Scomparsa REvil: merito di chi? Le 3 teorie

Il NYT elenca tre teorie principali sul motivo per cui **REvil** è improvvisamente scomparso. La prima è che Biden abbia ordinato al **Cyber Command** degli Stati Uniti, in collaborazione con le forze dell'ordine nazionali, incluso l'FBI, di chiudere i siti del gruppo.

La seconda teoria è che Putin abbia ordinato la rimozione dei siti del gruppo. Se così fosse, sarebbe un gesto per dare ascolto all'avvertimento di Biden avvenuto durante l'incontro dei due leader di Ginevra.

Continua a leggere l'articolo su Cybersecurity Italia, su cui è stato originariamente pubblicato.

https://www.key4biz.it/ransomware-revil-il-gruppo-criminal-hacker-piu-pericoloso-al-mondo-e-scomparso-dal-web/368465/