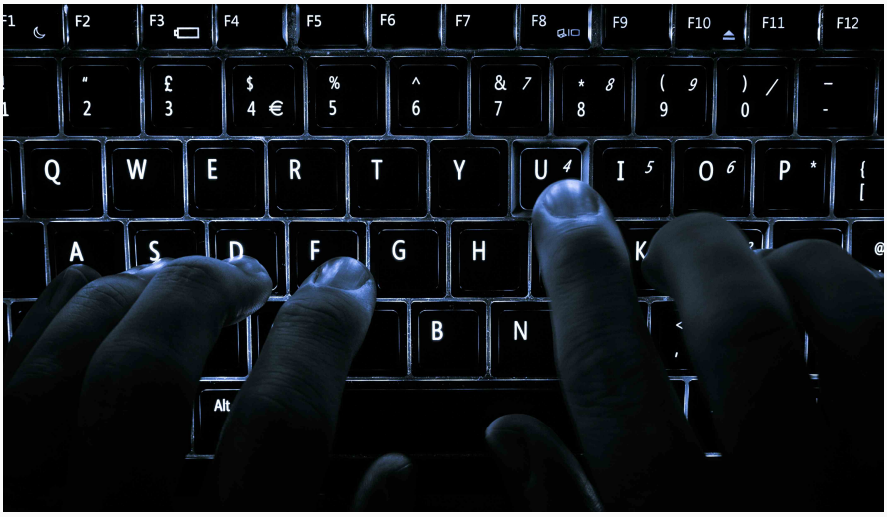
IL CASO

Attacco hacker Lazio, D'Amato: "E' partito dall'utenza di un dipendente in smart working"

L'annuncio dell'assessore alla Sanità mette un punto fermo sulla natura della violazione ai sistemi informativi della Regione, che da domenica blocca numerosi servizi. La procura indaga per associazione con finalità di terrorismo o di eversione dell'ordine democratico

03 Ago 2021



Quel che è certo è che tutto è partito dalla "**violazione di un'utenza di un dipendente in smart working**", ovvero "in un momento particolare, quando il livello di attenzione si

Argomenti trattati

Personaggi
- Alessio D'Amato
- Luciana Lamorgese
- Mario Draghi
- nicola zingaretti
- Sergio Mattarella

Aziende
- Cnr
- commissione ue
- copasir
- Garante protezione dati
- regione lazio

Approfondimenti
- attacco
- campagna vaccinale
- covid-19
- cyberattacco
- hacker
- Ransomware
- regione lazio
- smartworking
- vulnerabilità

abbassa". L'**assessore alla Sanità del Lazio, Alessio D'Amato,** mette un primo vero punto fermo dopo il massiccio **attacco hacker – di matrice terroristica – che da domenica paralizza con ripetuti attacchi i sistemi informatici della Regione, con una mira particolare alle operazioni di vaccinazione anti Covid.** E spiega, in particolare, che "sono state cambiate le chiavi della porta che fa accedere al **Ced**, il sistema che gestisce i dati sanitari, le pratiche edilizie e molti servizi al cittadino".

E' dunque sulla **cybersicurezza** che si trasferisce ora il dibattito politico innescato dall'episodio. E mentre **Zingaretti e D'Amato** chiedono che si faccia in fretta ("Dobbiamo correre sulla cybersecurity perché una parte d'Italia è già nella dimensione digitale, forse grazie anche al Covid", ha puntualizzato il presidente regionale), la priorità ora resta l'**emergenza**. La "conta dei morti" lascia (per ora) sul campo dati immobilizzati per giorni a causa del backup criptato, ritardi nel rilascio del Green pass, pagamenti di bolli auto e ticket, prenotazioni di visite specialistiche ambulatoriali e molti altri servizi telematici pubblici completamente bloccati, ma per fortuna nessuna violazione dei dati personali degli utenti e nessun disagio alla rete di emergenza e urgenza (ovvero tutti i servizi di natura ospedaliera, degenze, servizi 118, 112, pronto soccorso e trasfusionale). E presto, **al massimo entro 72 ore secondo gli annunci, si torna alla normalità anche nelle prenotazioni alla campagna vaccinale.** "Siamo in guerra, come sotto un bombardamento. Si contano gli edifici che stanno in piedi e quelli che sono crollati, ma chi aveva una prenotazione può recarsi tranquillamente al centro vaccinale: le somministrazioni non si sono mai interrotte. Per chi invece deve prenotare, tra 72 ore sarà pronta una nuova modalità". ha puntualizzato l'assessore.

Indice degli argomenti

Criptato il backup dei dati, ma nessuna violazione delle informazioni sensibili

La gravità dei fatti ha imposto un massiccio e tempestivo dispiegamento di forze inquirenti e operative, grazie al quale è stato possibile far fronte alle maggiori criticità in tempo breve: "Si sta

Articoli correlati

CYBERSECURITY
Regione Lazio sotto attacco hacker, Zingaretti: "Azione terroristica"
02 Ago 2021

IL BANDO
Pmi, dalla Regione Lazio 5 milioni per il voucher "diagnosi digitale"
29 Lug 2021

PA DIGITALE
Lazio e Emilia-Romagna spingono sul riuso: in condivisione l'archivio informatico
27 Lug 2021

L'ANALISI
Smart Working, Gartner: "Un dipendente su 10 tenterà di aggirare i controlli"
09 Feb 2021

lavorando giorno e notte", ha confidato il **presidente della Regione, Nicola Zingaretti,** ammettendo che le violazioni si sono susseguite anche la scorsa notte. Risultato: il problema della **refertazione dei tamponi per il Covid**, ad esempio, "è stato affrontato e risolto: tutte le farmacie, adesso, registrano l'esito direttamente sulla tessera sanitaria e così è **possibile ottenere il green pass**", ha chiarito **D'Amato**. "Crediamo che prima di Ferragosto saremo in grado di far ripartire almeno per una buona parte dei servizi alla popolazione regionale, come le prenotazioni per i vaccini, anche perché era già in corso una trasmigrazione verso un nuovo cup, ovvero la centrale unica delle prenotazioni – ha aggiunto -. **Rimane però una problematica più ampia per altre parti, dove i tempi sono più lunghi**".

Indagini per terrorismo: il Lazio possiede dati delle più alte cariche dello Stato

D'Amato ha spiegato che "l'elemento più grave" dell'attacco è rappresentato dalla crittografia "del backup dei dati, che tuttavia non sono stati violati ma solo immobilizzati". Alla luce dei fatti**, la**

CONFERENZA DELLE REGIONI E DELLE PROVINCE AUTONOME
CORCOM
www.corrierecomunicazioni.it
Utenti unici: 10.189
Rassegna del 03/08/2021
Notizia del: 03/08/2021
Foglio:4/6

Procura ha aperto un fascicolo ipotizzando i reati di associazione con finalità di terrorismo o di eversione dell'ordine democratico. L'indagine è coordinata dal pool dei reati informatici ma anche da quello dell'antiterrorismo.

La decisione è arrivata dal **capo della procura di Roma, Michele Prestipino**, considerando che l'attacco ha coinvolto un sistema importante e complesso come quello della **Regione Lazio**, esponendo a **rischio diffusione dati sensibili di varie personalità dello Stato, come, ad esempio, il presidente della Repubblica, Sergio Mattarella e il presidente del Consiglio, Mario Draghi, che proprio a Roma si sono vaccinati.** Nel fascicolo si procede contro ignoti per diversi reati tra cui accesso abusivo a sistema informatico e tentata estorsione. A coordinare gli accertamenti sarà il procuratore aggiunto, **Angelantonio Racanelli.**

Le reazioni della politica: audizioni con il Copasir

Intanto, sulla questione si sta muovendo anche il mondo politico. Per oggi è stato **convocato il Comitato parlamentare per la sicurezza della Repubblica per l'audizione del ministro dell'Interno, Luciana Lamorgese.** L'audizione era già prevista e sarebbe dovuta essere l'ultima prima della pausa estiva. Oltre alla titolare del **Viminale, il Copasir** ha però ritenuto necessario di svolgere domani alle 14 anche un'audizione del **direttore del Dis, l'ambasciatore Elisabetta Belloni,** per avere ulteriori elementi in merito al grave attacco informatico.

Una prima notizia in merito è arrivata ieri dal **presidente della Regione, Nicola Zingaretti,** il quale ha chiarito che "**nessuna richiesta di riscatto è stata avanzata**", anche se la Regione si trova di fronte comunque a "di uno dei più seri attacchi nella nostra Repubblica contro la pubblica amministrazione".

Martinelli (Cnr): "Ecco come funziona un ransomware"

Fabio Martinelli, dirigente di ricerca dell'Istituto di informatica e telematica del Cnr e co-referente per l'area progettuale in cyber security, dà invece una lettura tecnica dei fatti, spiegando che il **ransomware** – ovvero lo strumento di hacking utilizzato per la violazione – "è un software malevolo che andando in esecuzione su

CONFERENZA DELLE REGIONI E DELLE PROVINCE AUTONOME
CORCOM
www.corrierecomunicazioni.it
Utenti unici: 10.189
Rassegna del 03/08/2021
Notizia del: 03/08/2021
Foglio:5/6

sistemi informatici li rende inservibili fintanto che un riscatto (ransom) è pagato, tipicamente in bitcoin una moneta virtuale (o critto valuta) facilmente trasferibile e difficilmente rintracciabile (di fatto permettendo a criminali dall'altra parte del mondo di attaccare i nostri sistemi e ricevere un compenso senza spostarsi dalla propria scrivania). Tipicamente **il ransomware agisce cifrando con una chiave ignota al possessore del Sistema informatico stesso, i files (dati) presenti, rendendoli inservibili da parte del legittimo proprietario**. Se la cifratura è fatta con algoritmi robusti, sarà poi praticamente impossibile da parte del proprietario in tempi brevi riavere accesso ai files originali".

"In genere, comunque **i ransomware non diffondono fuori del sistema informatico i dati del sistema stesso** – aggiunge -, rendendo il ransomware tipicamente un caso di mancata disponibilità dei dati e non di confidenzialità dei dati stessi". Per mitigare questo attacco vi sono varie soluzioni: "Quella tipica – chiarisce **Martinelli** – è creare regolarmente delle **copie di backup o ripristino, che dovrebbero essere utilizzate nel caso i file originali non siano disponibili.** E' però importante **assicurarsi che le copie di back-up non siano suscettibili del medesimo attacco, come purtroppo sembra sia successo nel caso della Regione Lazio.** In questo caso il ripristino allo status quo può risultare molto difficile se non impossibile. Altre soluzioni sono ovviamente avere dei programmi di in esecuzione nei sistemi stessi rilevano la presenza del malware (antivirus) e gli usuali meccanismi di autenticazione che sono in essere in questi sistemi".

E, mettendo l'accento sull'importanza della **cybersecurity**, conclude: "L'attacco alla **Regione Lazio** fa risaltare una serie di dati noti. La **diffusione delle smart working (che è stata fondamentale per rendere resiliente il Sistema paese) rende anche più vulnerabili i sistemi informatici,** in quanto si compie un accesso da una serie di computer e device più deboli e inseriti in un contesto meno difendibile quello familiari con molti device non protetti".

Polizia postale: "Attacchi alle nostre infrastrutture lievitati del 246% in un anno"

CONFERENZA DELLE REGIONI E DELLE PROVINCE AUTONOME
CORCOM
www.corrierecomunicazioni.it
Utenti unici: 10.189
Rassegna del 03/08/2021
Notizia del: 03/08/2021
Foglio:6/6

Ad aggiungere un tassello al quadro è anche **Nunzia Ciardi, direttore della polizia postale e delle comunicazioni,** la quale puntualizza che "il crimine digitale non ha le classiche delimitazioni. La Rete ha travolto i confini, tanto più che **gli attacchi vengono commessi in una realtà transnazionale,** con la sovrapposizione di diversi sistemi legislativi e differenti norme sul trattamento dei dati. Fondamentale è la collaborazione internazionale". Il direttore, in un'intervista a *La Stampa*, ha fatto anche presente che "negli ultimi anni **gli attacchi cyber sono aumentati moltissimo**, sia per motivi di natura storica, nel senso che stiamo diventando sempre più una società a carattere digitale, sia a causa del Covid. La pandemia ha infatti impresso un'accelerazione a un settore che era già in salita. Tra smart working, didattica a distanza, spesa online è aumentato a dismisura il numero delle operazioni nel web e questo ci ha reso più esposti e più vulnerabili. Anche perché navighiamo con connessioni non sicure". "**Dal 2019 al 2020 – ha fatt notare – gli attacchi alle infrastrutture del nostro Paese sono lievitati del 246%.** E non va bene neanche per pedopornografia e adescamenti online, con crescite del 130%".

Sguardi puntati sulla vicenda

Il **Garante per la protezione dei dati personali**, intanto, segue "con particolare attenzione – come chiarito in una nota ufficiale – gli sviluppi dell'attacco informatico subito dalla **Regione Lazio**, con la quale ha preso subito contatti per tutto quanto attiene agli aspetti di protezione dei dati personali degli interessati coinvolti nel **data breach**. La Regione ha fatto pervenire una prima notifica preliminare di violazione dei dati all'Autorità, la quale si riserva di **valutare a pieno la situazione una volta ricevuti ulteriori elementi anche all'esito delle analisi che la Regione sta compiendo**".

E una portavoce della **Commissione europea**, durante l'incontro con la stampa a **palazzo Berlaymont**, ha concluso: "Abbiamo visto le notizie stampa sull'attacco informatico al portale sanitario e per le vaccinazioni della **Regione Lazio**. **Prendiamo la cosa molto sul serio**".