ATTUALITÀ

Attacco cibernetico alla Regione Lazio: cos'è davvero successo?

di **Fondazione AIDR** · 11 ottobre 2021, 21:38

di Giuseppe Gorga, socio Aidr

Aumentano gli attacchi alle reti informatiche delle aziende e degli enti pubblici. Recente caso clamoroso, è quello dell'attacco alla Regione Lazio ad inizio agosto 2021.Indagano anche Cia e Europoll

La gestione del rischio di attacchi infomatici non è sempre semplice, poiché la cybercriminalità evolve competenze e capacità di pari passo all'innovazione dei sistemi integrati di protezione delle banche dati virtuali e dei sistemi informatici.Recente caso emblematico, infatti, è rappresentato dall'attacco hacker alla Regione Lazio nei primi del mese di agosto dell'anno corrente.

Secondo indiscrezioni iniziali, l'attacco che ha paralizzato i sistemi informatici della Regione Lazio sarebbe originato dal computer di un dipendente della società Engineering.La smentita da parte di Engineering è arrivata immediatamente tramite una nota attraverso cui la Società ha fatto sapere di non aver ricevuto alcuna notifica da parte degli inquirenti rispetto a possibili collegamenti con l'evento, e che se nel corso di verifiche si evidenziasse qualcosa di diverso, saranno loro stessi ad inoltrare notifica alle autorità competenti.

Sul caso, collaborano alle indagini anche Fbi e Europol. L'attacco è partito in data al CED regionale. I sistemi informatici sono stati tutti disattivati compresi tutti quelli del portale Salute Lazio e della rete vaccinale. Il CED gestisce i dati sanitari e personali di circa sei milioni di cittadini ed i sistemi informatici che consentono di portare avanti la campagna regionale di vaccinazione contro il coronavirus.

Dopo alcuni giorni di sospensione, il sistema della Regione Lazio per la prenotazione dei vaccini è stato ripristinato, ma rimane l'allerta per eventuali nuovi attacchi.

Sembra che il “cryptolocker” utilizzato abbia reso inutilizzabili anche i dati presenti nel backup, e che la Regione Lazio sia solo il quarto soggetto coinvolto in questo attacco. Secondo altre fonti, sembra che l’accesso sia avvenuto durante una sessione amministrativa lasciata in log-in da un dipendente di Lazio Crea, pertanto sembra essere stato un attacco ransomware, detto anche “supply-chain”.

L’analisi del link Tor lasciato dai criminali ha rivelat oche il malware è RansomExx. È impiagato da un gruppo cybercriminale già noto per violazioni di diversi Governi e grandi aziende. Sembra che il computer del dipendente di Frosinone da cui è partito l’attacco sia stato contagiato da malware. A causa di errori di gestione privilegi o di password in Regione, è molto probabile sia stato possibile per i cybercriminali passare dal computer del dipendente ad account con privilegi di amministratori, con cui criptare il sistema. Sfruttando queste vulnerabilità, o in presenza di errori di proggettazione della security del sistema, infatti, è possibile ottenere privilegi d’accesso ed avere in mano il controllo dei dati posseduti (Nevacci, 2021).

Nel caso di specie, non si è trattato di un attacco di tipo ideologico (dato il coinvolgimento dei dati sulle vaccinazioni, si è ipotizzato che fosse stato promosso dalla corrente “no-vax”) quanto, piuttosto, di un attacco di tipo puramente estorsivo, con l’unico obiettivo di trarre un vantaggio economico. La procura di Roma ha formulato per questi episodi i reati di accesso abusivo ad un sistema informatico, tentata estorsione e danneggiamento di sistemi informatici, con l’aggravante della finalità del terrorismo. A coordinare le indagini sono il procuratore capo e vertice del pool dei reati informatici, Michele Prestipino e il procuratore aggiunto, Angelantonio Racanelli, impegnato nella lotta ai reati connessi al terrorismo.

È intervenuta immediatamente sul caso anche la Ministra dell’interno Luciana Lamorgese, che ha parlato in occasione di un discorso al Copasir di “recrudescenza del fenomeno, che negli ultimi mesi ha colpito sia attività pubbliche che private” ed ha rilevato “la necessità di agire con urgenza per elevare il livello di sicurezza, la resilienza dei sistemi informatici e l’istruzione degli operatori”.

Il mantenimento di idonei standard di sicurezza informatica sta generando un fabbisogno crescente di e-lawyers ed esperti informatici, quali profili fondamentali per la protezione dei portali informatici, la tutela dei dati sensibili e la risoluzione di eventuali controversie. (Lupària & Ziccardi, 2007).

Sull’onda del fabbisogno di queste nuove skills, recentemente sono aumentate in Italia le offerte formative professionalizzanti che puntano a creare in uscita figure esperte nella gestione della sicurezza informatica. La nascita di nuove offerte formative rappresenta una modello di risposta

necessario per dare alle istanze sorte in capo ai recenti accadimenti e dei dispositivi normativi qui citati, poiché partecipano a pieno titolo alla formazione di profili essenziali per la soluzione delle problematiche che in maniera ricorrente si presentano nel campo della sicurezza informatica. Pertanto sarà necessario che i decisori politici, nazionali ed extranazionali, attivino misure che incentivano gli enti di formazione professionale del comparto sicurezza informatica.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/10/11/attacco-cibernetico-alla-regione-lazio-cose-davvero-successo/

© 2026 Istituzioni24