6 agosto 2021 9:24

L'attacco hacker alla Regione Lazio. Il giorno dopo

di Redazione

Ho aspettato un po' a scrivere di questa vicenda per lasciare che si depositasse il polverone delle dichiarazioni politiche e cominciassero a emergere i fatti tecnici. I fatti sono ancora pochi, comunque, ed è piuttosto evidente a questo punto che non c'è alcuna intenzione delle autorità di fare piena chiarezza sulla vicenda. Prendete quindi queste poche righe con beneficio d'inventario.

Quello che si sa per certo, finora, è che i servizi informatici della Regione Lazio sono offline da domenica 1 agosto. Secondo la ricostruzione de Il Post (anche qui), un ransomware ha colpito il centro elaborazione dati (CED) che gestisce tutta la struttura informatica regionale e i tecnici hanno pertanto disattivato il CED.

Questo ha portato quasi alla paralisi tutti i servizi regionali che dipendono dal CED, fra i quali spicca il servizio di vaccinazione contro il Covid (che sta procedendo lentamente usando un sistema cartaceo ma ha le prenotazioni bloccate).

Il presidente della Regione Lazio, Nicola Zingaretti, ha parlato di difesa contro "attacchi criminali o di stampo terroristico" (sottolineo "o"), ma ANSA ha inventato un virgolettato che gli ha messo in bocca una certezza sullo stampo terroristico che di fatto Zingaretti non ha espresso (perlomeno nello spezzone video riportato nel tweet di ANSA).

I giornali generalisti italiani si sono lanciati in narrazioni che per pietà mi limito a definire fantasiose, per cui non è opportuno considerare affidabile qualunque affermazione informatica scritta da queste testate e conviene rivolgersi solo a fonti tecniche qualificate.

Per quello che è dato sapere fin qui, non c'è nessuna evidenza di un attacco di stampo terroristico: sembra invece trattarsi di un classico attacco criminale, effettuato a scopo di estorsione. Un tipico ransomware, insomma, di quelli che colpiscono tutti i giorni tante aziende: i dati vengono cifrati dai criminali, che poi chiedono il pagamento di un riscatto per avere la chiave di decifrazione. Stavolta il bersaglio è un po' più grosso e il danno è molto più visibile.

L'ipotesi del terrorismo informatico è altamente improbabile perché un attacco a fini terroristici avrebbe semplicemente cancellato i dati invece di cifrarli, come ha giustamente fatto notare Stefano Zanero, professore associato di Computer Security al Politecnico di Milano.

Ieri è stato diffuso uno screenshot, parzialmente oscurato, che mostrerebbe l'avviso del ransomware, con un link a una pagina del dark web da usare per la trattativa con gli esecutori dell'attacco.

Secondo BleepingComputer, il link alla pagina è collegato a un gruppo di criminali informatici noto come RansomEXX, che ha già preso di mira grandi aziende in vari paesi del mondo, e la tecnica di attacco del gruppo consiste nel violare le difese di una rete aziendale usando delle vulnerabilità o delle credenziali rubate, per poi scorrazzare nella rete rubando o cifrando file e prendere il controllo del domain controller Windows per diffondere il software di cifratura su tutta la rete.

Gli attacchi di ransomware di solito agiscono su due fronti fondamentali di monetizzazione: la minaccia di bloccare l'attività della vittima e la minaccia di disseminare i dati custoditi dalla vittima (con conseguenti disagi e danni).

Zingaretti ha dichiarato che "nessun dato sanitario è stato rubato e i dati finanziari e del bilancio non sono stati toccati" (Il Post), ma è decisamente troppo presto per essere così categorici.

Per ora, quindi, le domande superano ampiamente le risposte.

Come è stato possibile un attacco del genere? Secondo le informazioni pubblicate da Open, l'attacco sarebbe iniziato prendendo di mira un PC di un dipendente di Lazio Crea, "società controllata dalla Regione, in smartworking a Frosinone. Per entrare nel sistema, come hanno spiegato fonti della polizia postale a Repubblica, i pirati hanno bucato Engineering SPA [sic], la società specializzata in servizi informatici che lavora con molte amministrazioni pubbliche [...] Da lì hanno ottenuto le credenziali dell'impiegato di Lazio Crea, che aveva i privilegi di amministratore. Hanno inserito il ransomware nel sistema informatico ed è partita la copia dei file." Uno schema assolutamente classico, insomma. Engineering SPA (in realtà Engineering Ingegneria Informatica S.p.A.) ha però preso posizione su questa ricostruzione degli eventi.

Non si possono ripristinare i dati da un backup? Non è così semplice. Come regola generale, prima di tutto bisogna assicurarsi che la rete informatica sulla quale si va a ripristinarli sia pulita e non contenga ancora il ransomware, altrimenti è tempo sprecato. Occorre quindi ripulire la rete oppure crearne una nuova vergine (cosa non facile per sistemi informatici grandi e complessi come un CED regionale). Poi bisogna avere un backup, e questo backup deve essere recente e pulito. Ma a quanto risulta dalle dichiarazioni di un assessore della Regione Lazio, almeno parte dei backup era tenuta in linea e quindi sarebbe anch'essa cifrata. Un altro errore classico. Tenere offline un backup integrale di grandi database non è semplice, certo, ma non farlo è una negligenza imperdonabile.
Come si possono evitare disastri del genere? Anche questo non è facile, ma i passi da compiere per ridurre la possibilità che accadano sono ben conosciuti:
ridurre la superficie di attacco, per esempio togliendo gli accessi privilegiati a chi non ne ha strettamente bisogno (in smart working o meno) e dandoli soltanto a chi ha macchine molto protette e non usate in modo promiscuo (no, il PC del dirigente sul quale guarda il sitarello porno o i film piratati non deve avere accesso privilegiato alla rete aziendale);
- predisporre una procedura di backup (che va collaudata e testata) che offra il massimo isolamento fisico possibile;
- predisporre un piano di disaster management per sapere cosa fare se (anzi quando) un attacco va a segno e in base a quanto va a segno;
- avere un piano di comunicazione chiaro e trasparente.

Fra queste soluzioni, noterete, è vistosamente assente qualunque accenno a grandiosi piani di "cloud nazionale". Perché "cloud nazionale" in politichese si traduce "pioggia di soldi per gli amici", ma in informatica si traduce "single point of failure". E se qualcuno ha bisogno che gli si traducano queste parole inglesi, tenetelo lontano da qualunque decisione informatica.

(Paolo Attivissimo su Zeus News)