Attacco hacker a Regione Lazio: Martinelli (Cnr), "necessari maggiori investimenti nella cybersecurity"

“Il ransomware è un software malevolo che andando in esecuzione su sistemi informatici li rende inservibili fintanto che un riscatto (ransom) è pagato, tipicamente in bitcoin, una moneta virtuale (o criptovaluta) 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)”. Lo spiega Fabio Martinelli, dirigente di ricerca dell’Istituto di informatica e telematica del Cnr e co-referente per l’area progettuale in cyber security, a proposito dell’attacco hacker alla Regione Lazio. “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, rendendo il ransomware tipicamente un caso di mancata disponibilità dei dati e non di confidenzialità dei dati stessi, aggiunge l’esperto. Per mitigare questo attacco “vi sono varie soluzioni: quella tipica è creare regolarmente delle copie di back-up o ripristino, che dovrebbero essere utilizzate nel caso i file originali non siano disponibili. Però, è 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 riprestino allo status quo può risultare molto difficile se non impossibile. Altre soluzioni sono ovviamente avere dei programmi di esecuzione nei sistemi stessi che rilevano la presenza del malware (antivirus) e gli usuali meccanismi di autenticazione che sono in essere in questi sistemi. Purtroppo anche se vari livelli di meccanismi di sicurezza sono presenti, i cybercriminali studiano continuamente dei meccanismi per superarli e renderli inefficaci”. In Italia, precisa Martinelli, “le attività in cybersecurity sono in rapida crescita con un notevole impegno del sistema governativo, industriale della formazione e della ricerca. A livello governativo è in dirittura d’arrivo l’iter per l’Agenzia per la cybersicurezza nazionale (Acn), che l’Italia attendeva da tempo. Anche il Cnr con i suoi istituti e con il laboratorio virtuale in cybersecurity contribuisce alle attività di ricerca e innovazione, partecipando a vari progetti di ricerca europei come ad esempio il centro di competenza europeo Sparta oppure Cyber4.0 a livello italiano, giusto per citarne alcuni che mettono insieme competenze pubbliche e private”. Per l'esperto, "la cybersecurity deve ricevere maggiori investimenti, come la presidente delle Commissione europea ha recentemente evidenziato, descrivendo la cyber security come l'altra faccia della medaglia della transizione digitale".

Gigliola Alfaro