Consiglio Nazionale delle Ricerche

A cura di Fabio Martinelli, dirigente di ricerca dell’Istituto di informatica e telematica del Cnr e co-referente per l’area progettuale in cybersecurity

Roma, 4 agosto 2021 - 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).

Tipicamente il ransomware agisce cifrando con una chiave ignota al possessore del Sistema informatico stesso, i file (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 file originali.

In
genere, comunque, i ransomware non diffondono fuori dal 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.

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. È 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 in 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.

L’attacco alla Regione Lazio fa risaltare una serie di dati noti. La diffusione dello 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 devices più deboli e inseriti in un contesto meno difendibile di quello familiare con molti devices non protetti.

Il dato di fatto è che i sistemi informativi della pubblica amministrazione in generale siano vulnerabili ad attacchi informatici di vario tipo come ha evidenziato una recente ricerca. Nel *cybercrime as a service* (crimine informatico come servizio) anche persone con limitata competenza possono acquisire strumenti per attaccare terze parti, e quindi le motivazioni dell'attacco possono andare da quelle economiche a quelle politiche.

In

Italia, 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 di 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.

Ma è del tutto evidente per il ruolo che la trasformazione digitale sta avendo e avrà che la cybersecurity debba ricevere maggiori investimenti, come la Presidente della Commissione europea ha recentemente evidenziato, descrivendo la cybersecurity come l'altra faccia della medaglia della transizione digitale.