Sono aumentati gli attacchi informatici contro le aziende energetiche

Il nucleo per la cybersicurezza (NSC), un organo governativo italiano che ha il compito di prevenire e risolvere gravi crisi di sicurezza informatica, si è riunito venerdì in seguito a due attacchi informatici contro due grosse aziende italiane che si occupano di energia: Eni e GSE, il Gestore dei servizi energetici italiano, una società partecipata interamente dal ministero dell'Economia. Al termine della riunione, l'agenzia nazionale per la cybercisurezza ha detto che c'è stato un aumento generalizzato degli attacchi informatici e che l'Italia risulta essere un «target particolarmente colpito».

Nell'ultimo anno in molti paesi diverse aziende energetiche sono state attaccate dai criminali informatici soprattutto con attacchi *ransomware*, un software che consente di rubare dati e tenerli bloccati con l'obiettivo di chiedere un riscatto. Un *ransomware* è un programma che, una volta installato in un sistema informatico, lo rende inaccessibile al proprietario tramite un sistema crittografico. Per poter accedere nuovamente ai dati, l'istituzione, l'azienda o la persona colpita deve pagare ai criminali un riscatto, spesso richiesto in criptovalute per garantire l'anonimato degli estorsori.

Sono attacchi molto efficaci che causano ingenti danni. Non servono grandi strumenti per organizzarli e consentono ai criminali di rischiare poco perché risalire agli autori è piuttosto complicato. I criminali informatici prediligono i bersagli più vulnerabili, cioè le attività che non possono rimanere bloccate per molto tempo come i fornitori di energia e le aziende sanitarie, due settori in cui è stato segnalato

un significativo aumento degli attacchi.

Uno dei casi più noti coinvolse Colonial Pipeline, uno dei più grandi e importanti oleodotti degli Stati Uniti, costretto a pagare 75 bitcoin (che al momento del pagamento valevano 4,4 milioni di dollari) per permettere la ripresa delle attività dell'oleodotto, bloccate a causa dell'attacco *ransomware*.

— Leggi anche: I criminali informatici sono diventati imprenditori

L'attacco contro Eni, la principale società energetica italiana, è stato segnalato mercoledì 31 agosto. «Eni conferma che nei giorni scorsi i sistemi di protezione interni hanno rilevato accessi non autorizzati alla rete aziendale», ha detto un rappresentante dell'azienda a *Bloomberg*. Secondo le ricostruzioni, l'attacco avrebbe causato danni lievi.

L'attacco a GSE, invece, era stato segnalato nella notte tra domenica 28 e lunedì 29 agosto ed è stato rivendicato dal gruppo criminale BlackCat, noto anche come ALPHV. GSE ha spiegato di aver isolato tempestivamente le infrastrutture informatiche, disattivando tutti i servizi telematici, le postazioni di lavoro e la posta elettronica. Del caso si è occupata anche l'agenzia nazionale per la cybersicurezza. «Non è da escludere che il grave attacco subito possa aver coinvolto dati personali e particolari nella titolarità del GSE a qualsivoglia titolo», ha chiarito GSE.

Come rilevato dall'NSC durante la riunione di venerdì, uno dei pericoli maggiori è rappresentato dalla diversificazione degli obiettivi dei gruppi criminali, che attaccano non solo le principali aziende, ma anche i fornitori più o meno grandi per colpire tutta la catena di approvvigionamento e distribuzione dell'energia.

I tecnici dell'NSC, in collaborazione con le altre agenzie europee e internazionali che si occupano di cybersicurezza, hanno alzato i livelli di protezione delle infrastrutture

digitali degli operatori energetici attraverso una serie di linee guida e raccomandazioni che i responsabili delle aziende dovranno seguire per prevenire nuovi attacchi. La minaccia è comunque difficile da evitare, perché negli ultimi anni i proventi degli attacchi hanno garantito uno sviluppo notevole dei ransomware e in generale del modello estorsivo.

Read More