Direttore: Carlo Verdelli
Audipress: n.d.

Repubblica Scienze

04-LUG-2019
da pag. 8

Pirateria informatica

Cybersicurezza, l'Italia è un colabrodo a rischio dighe e scambi ferroviari • a pagina 8

di **Rosita Rijtano**

IL RAPPORTO

Cyberguerra colabrodo Italia

Un giovane ricercatore informatico ha dimostrato l'estrema vulnerabilità dei sistemi di controllo industriali. Dai semafori alle ferrovie, tutto è facilmente attaccabile. E nessuno si preoccupa

Un paio d'anni fa in Gran Bretagna computer degli ospedali bloccati da un virus

di **Rosita Rijtano**

È il 24 giugno 2030, Roma: è tarda sera e d'improvviso tutti i semafori della città si spengono per via di un blackout, generando una catena di incidenti mortali. È solo uno dei tanti scenari plausibili leggendo una ricerca che svela la vulnerabilità dell'Italia a un'eventuale cyberguerra. Un'analisi che anticipa il futuro e mette in guardia sulla facilità con cui le nostre infrastrutture critiche potrebbero diventare bersaglio di un attacco informatico in grado di mandare in tilt l'intera nazione. Di paralizzare il traffico o gli ospedali, come accaduto in Gran Bretagna nel 2017 quando i computer dei nosocomi inglesi furono inchiodati da WannaCry: un virus che rende inaccessibili i dati delle macchine infette chiedendo il pagamento di un riscatto per ripristinarli. Il nuovo studio punta i riflettori su un particolare anello debole: quelli che tecnicamente vengono definiti sistemi di controllo industriale. In pratica, si tratta di computer che svolgono solo delle funzioni ben determinate, tanto specifiche quanto cruciali. Li troviamo a regolare l'aria condizionata degli uffici e dei centri commerciali, a controllare le turbine delle centrali idroelettriche, a gestire i deviatoi ferroviari o il livello dell'acqua all'interno delle dighe, e ad occupare posti chiave nelle catene produttive delle grandi aziende. «Dei dispositivi che non dovrebbero essere connessi alla Rete», dice Paolo Stagno, ricercatore di sicurezza informatica ventiseienne e autore dell'analisi. Invece, lo sono. Connetterli consente di controllarli e monitorarli da remoto, ma li rende anche a portata dei criminali informatici al soldo di uno Stato nemico. Usando Shodan, uno strumento che permette di riconoscere il tipo di dispositivi online tramite gli specifici protocolli utilizzati per comunicare, Stagno ha individuato 3630 di queste macchine in 264 città del nostro paese. La maggior


Rep
Scienze
La città bollente


Cyberguerra colabrodo Italia

Direttore: Carlo Verdelli
Audipress: n.d.

Repubblica Scienze

04-LUG-2019
da pag. 8

parte si concentra nell'Italia settentrionale, con la Lombardia che conquista il primato grazie al 22 percento dei sistemi di controllo industriale connessi a internet, seguita da Piemonte, Emilia Romagna, Friuli Venezia Giulia e Lazio. La loro funzione esatta è impossibile da stabilire, se non infrangendo la legge. Ma l'indicativa collocazione geografica cui si può risalire tramite l'indirizzo IP, cioè quell'etichetta numerica che identifica univocamente un dispositivo collegato alla Rete, permette di farsi un'idea su luogo e modalità d'utilizzo.

Sono collocati in alcuni importanti complessi industriali del nostro paese, nelle stazioni ferroviarie, nelle centrali elettriche e persino nelle dighe. Tutti servizi essenziali che possono essere facilmente hackerati. Si ha l'opportunità non solo di alterare il funzionamento del singolo computer, deviando per esempio un treno su un binario sbagliato. Ma anche di compromettere l'intero sistema, con importanti conseguenze. Come lasciare le città italiane senza elettricità. «Ognuno di loro si trova all'interno di una Rete critica e potrebbe servire da punto d'entrata. Come dei piccoli cavalli di Troia», spiega Davide del Vecchio, responsabile della sicurezza informatica di Deltatre. Un problema destinato a crescere man mano che sempre più oggetti finiscono online.

Stefano Chiccarelli, protagonista dell'informatica italiana, conosce bene la situazione descritta dalla ricerca. È amministratore delegato di Quantum Leap, compagnia specializzata in test che valutano la vulnerabilità di un sistema a un attacco, e avverte: «C'è una totale mancanza di consapevolezza da parte di chi gestisce questo tipo di ambienti nei confronti della sicurezza. Quando, in realtà, sono loro a subire i principali danni».