

GUERRA IBRIDA, QUANTO SONO DAVVERO SICURE LE NOSTRE INFRASTRUTTURE?PARLA UNA AZIENDA INNOVATIVA DEI CASTELLI ROMANI di (ROMA)

default watermark

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Frigoriferi commerciali, ospedali, acquedotti e impianti industriali: la nuova frontiera degli attacchi informatici passa dai sistemi connessi. HyBiz CyberLab e Rogue Data presentano uno studio su 15.795 servizi Internet. Il 38,5% del campione analizzato presenta livelli di esposizione classificati come alti o critici. Lâ??intelligenza artificiale moltiplica la capacitÃ offensiva, ma puÃ² diventare anche uno strumento decisivo per la difesa.

La guerra ibrida non si combatte soltanto attraverso attacchi informatici ai sistemi istituzionali o alle grandi infrastrutture strategiche. Sempre piÃ¹ spesso il rischio passa da dispositivi apparentemente ordinari: telecamere, sistemi di refrigerazione commerciale, impianti industriali e apparati di controllo collegati alla rete.

Ã? quanto emerge da un nuovo studio tecnico-scientifico realizzato da HyBiz CyberLab, societÃ italiana specializzata in intelligenza artificiale, cybersecurity e infrastrutture tecnologiche, insieme alla consociata Rogue Data. La ricerca analizza un campione di 15.795 servizi di rete distribuiti su 9.935 indirizzi IPv4 pubblici distinti, con lâ??obiettivo di misurare il livello di esposizione dei sistemi Internet of Things (IoT) e Operational Technology (OT).

I numeri evidenziano una situazione che merita particolare attenzione: 6.084 servizi, pari al 38,5% del campione, rientrano nelle fasce descrittive di esposizione alta o critica. Inoltre, 3.336 indirizzi presentano almeno un pannello amministrativo raggiungibile pubblicamente.

Un dato significativo riguarda la refrigerazione commerciale: su 476 servizi individuati, 404, pari allâ??84,9%, espongono informazioni identificative del sistema prima ancora dellâ??autenticazione. Una condizione che puÃ² facilitare le attivitÃ di ricognizione da parte di soggetti interessati a individuare possibili punti di accesso.

Lo studio precisa che questi risultati non dimostrano lâ??avvenuta compromissione dei sistemi analizzati, ma individuano una superficie di esposizione che richiede verifiche e interventi di sicurezza prioritari.

Il problema assume una dimensione ancora piÃ¹ rilevante quando le tecnologie informatiche entrano in contatto con le infrastrutture che gestiscono processi fisici.

Nella grande distribuzione, ad esempio, i sistemi digitali possono controllare le temperature dei frigoriferi. In ambito sanitario e nei laboratori di ricerca, invece, la catena del freddo custodisce farmaci, vaccini, campioni biologici e sacche ematiche.

Un attacco informatico a questi sistemi puÃ² quindi produrre conseguenze che vanno ben oltre il danno economico, coinvolgendo la continuitÃ dei servizi e, nei casi piÃ¹ gravi, la sicurezza delle persone.

Particolarmente delicato Ã¨ anche il settore della distribuzione idrica. I sistemi industriali SCADA e i controllori digitali governano pompe, valvole e processi di trattamento dellâ??acqua. Unâ??alterazione dei parametri operativi negli impianti che utilizzano composti a base di cloro potrebbe determinare problemi di sotto-disinfezione o unâ??esposizione eccessiva ai reagenti, con potenziali conseguenze per la salute pubblica.

default watermark

Non si tratta soltanto di ipotesi teoriche. Un bollettino congiunto statunitense del dicembre 2024 ha documentato manomissioni delle interfacce di controllo di impianti idrici da parte di gruppi hacktivisti filorussi, con modifiche dei parametri operativi e il ricorso, da parte di alcuni gestori, al controllo manuale.

Uno degli aspetti centrali della ricerca riguarda il rapporto tra intelligenza artificiale e nuove minacce informatiche.

Per anni individuare apparati esposti, comprenderne le funzioni, riconoscere versioni software vulnerabili e costruire una campagna offensiva ha richiesto competenze tecniche, tempo e risorse considerevoli.

Oggi lâ??intelligenza artificiale permette di automatizzare diverse fasi di queste attivitÃ : dalla ricognizione delle infrastrutture alla classificazione dei dati, fino allâ??assistenza nella scrittura di codice e alla produzione di comunicazioni fraudolente sempre piÃ¹ credibili.

Questo scenario amplia la platea dei potenziali aggressori e aumenta lâ??efficienza di chi possiede giÃ competenze offensive. Il National Cyber Security Centre britannico, nel rapporto Annual Review 2026, descrive lâ??impatto dellâ??intelligenza artificiale sulle minacce informatiche come un vero moltiplicatore di forza.

Phishing mirato, deepfake, falsi allarmi, sabotaggi digitali e blocco dei processi operativi possono cosÃ¬ diventare componenti di strategie coordinate di guerra ibrida.

La risposta non puÃ² limitarsi agli strumenti tradizionali di protezione. Occorre sviluppare sistemi capaci di individuare tempestivamente le esposizioni, riconoscere le anomalie e monitorare costantemente le infrastrutture.

La ricerca propone un modello di osservazione e prevenzione basato sullâ??identificazione degli apparati esposti, sulla ricostruzione delle loro caratteristiche tecniche e sullâ??individuazione delle prioritÃ di intervento.

Il paper individua quattro principali misure di riduzione dellâ??esposizione: limitare i servizi visibili pubblicamente, proteggere le interfacce amministrative, eliminare le informazioni identificative accessibili prima del login e aggiornare i software obsoleti.

Secondo le simulazioni riportate nello studio, una combinazione di tre interventi consente di ridurre del 75,2% il numero di servizi collocati nelle fasce superiori dellâ??indice di esposizione.

Lâ??obiettivo Ã¨ arrivare a un osservatorio strutturato, inizialmente concentrato sullâ??area di Roma, capace di raccogliere informazioni sugli apparati installati, verificare la corrispondenza tra servizi Internet e dispositivi reali e sviluppare test autorizzati su campioni rappresentativi.

Lâ??intelligenza artificiale e gli agenti software possono supportare queste attivitÃ , mentre le verifiche intrusive e qualsiasi modifica agli impianti restano subordinate allâ??autorizzazione dei titolari e al controllo umano.

default watermark

Il progetto coinvolge competenze differenti nel campo della cybersecurity, dellâ??intelligenza artificiale e dello sviluppo di infrastrutture digitali.

Gustavo Mastrobuoni, legato a Rogue Data come CTO e responsabile della ricerca e sviluppo, ha maturato esperienze dirigenziali in Microsoft e KPMG. Si occupa da anni di eGovernment, cybersecurity, interoperabilitÃ , innovazione e ricerca applicata.

Marco Valerio Roscioni, founder di HyBiz, opera nello sviluppo di infrastrutture digitali, intelligenza artificiale e soluzioni immersive. In azienda segue la visione di prodotto e i sistemi di AI locale, con particolare attenzione alla proprietÃ e al controllo delle infrastrutture tecnologiche.

Gustavo Mancini contribuisce alla direzione tecnica e alla gestione di progetti digitali complessi, occupandosi dellâ??integrazione tra hardware, software e sistemi intelligenti.

Francesco Giuliani, lead developer, segue la progettazione e lo sviluppo software, le integrazioni e le componenti applicative di intelligenza artificiale.

Rogue Data dichiara collaborazioni e partnership operative con il Consiglio Nazionale delle Ricerche (CNR), con attivitÃ presso lâ??Area della Ricerca di Montelibretti e lâ??Istituto di Cristallografia, con ENEA e con lâ??UniversitÃ degli Studi di Roma Tor Vergata. Nel network indicato dallâ??azienda figura anche lâ??UniversitÃ degli Studi di Cassino e del Lazio Meridionale.

Le collaborazioni costituiscono il contesto scientifico e tecnologico di riferimento dellâ??azienda e non rappresentano una co-firma o una validazione del paper presentato.

La cybersecurity non puÃ² piÃ¹ essere considerata soltanto una questione di antivirus, firewall e password. La sicurezza digitale riguarda ormai la capacitÃ di mantenere operative le infrastrutture da cui dipende la vita quotidiana delle comunitÃ : acqua, energia, alimentazione, trasporti, sanitÃ e comunicazione.

La sfida dellâ??intelligenza artificiale sarÃ quindi anche una sfida di prevenzione, conoscenza e controllo delle tecnologie.

La differenza tra attaccare e difendersi non dipenderÃ soltanto dalla potenza dei sistemi, ma dalla velocitÃ con cui saremo capaci di individuare le vulnerabilitÃ , correggerle e governarle.

Contatti:
KTP.Agency
emiliano.stampa@gmail.com

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

default watermark

ResponsabilitÃ editoriale di KTP.Agency

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Novembre 20, 2026
Autore
redazione