Cybersecurity, a Roma 297mila dispositivi a rischio attacco hacker

A **Roma** sono 296.786 i dispositivi a rischio attacco cyber e, se si sommano i sistemi a rischio presenti nelle capitali dell'Europa occidentale, si arriva a un totale che supera i 10 milioni.

Tra i dispositivi a rischio si contano 217.109 web service, 2.890 email service, 2.595 webcam, 432 MySQL database, 154 router, 79 dispositivi VoIP e 29 registratori media. Questo è quello che emerge dall'ultimo report "Western European Cities Exposed" di Trend Micro.

Lo studio ha analizzato i cosiddetti "sistemi esposti" di 2,7 milioni di indirizzi IP in 10 capitali europee: Amsterdam, Atene, Berlino, Lisbona, Londra, Madrid, Oslo, Parigi, Roma e Stoccolma, ovvero quei dispositivi collegati a Internet che rispondo alle richieste sia tramite strumenti di gestione della rete o di enumerazione, come un ping, o che possono essere trovati da motori di ricerca internet come Shodan o simili. Non sono per definizione vulnerabili o compromessi, ma il fatto che siano connessi significa che possono essere attaccati in qualunque momento.

I dispositivi esposti offrono ai possibili attaccanti una radiografia di come i dispositivi stessi sono utilizzati dalle aziende e dai governi, questo può facilitare le operazioni di infiltrazione nella rete. I sistemi connessi a Internet spesso restano aperti a potenziali attacchi o perdite di dati perché non sono configurati correttamente. Tuttavia, alcuni devono essere connessi per forza a Internet, per poter funzionare correttamente o per abilitare l'accesso remoto per la risoluzione dei problemi e altre attività. I dispositivi a

rischio possono provocare una fuga di informazioni private all’insaputa dell’utente, permettere il furto di dati critici aziendali e governativi, essere sfruttati per attacchi mirati o attacchi DDoS e anche essere presi in ostaggio nel corso di un attacco ransomware.

Per quanto riguarda la tipologia dei dispositivi, lo studio ha rivelato che nelle città esaminate sono a rischio, in totale, 58.000 punti di accesso wireless, 34.000 firewall e 28.000 webcam. Inoltre è stato rilevato un grande numero di stampanti accessibili pubblicamente da internet, che mettono potenzialmente a rischio le copie di dati sensibili, così come offrono agli attaccanti un punto per entrare all’interno delle reti aziendali. I sistemi operativi esposti maggiormente sono Linux (62%) e Windows (20%).

Questo studio deve essere tenuto in particolare considerazione, anche in relazione all’entrata in vigore del **nuovo Regolamento Europeo sulla protezione dei dati (GDPR)**. I dispositivi a rischio innalzano infatti il rischio di subire una violazione di dati, severamente punita dal regolamento.