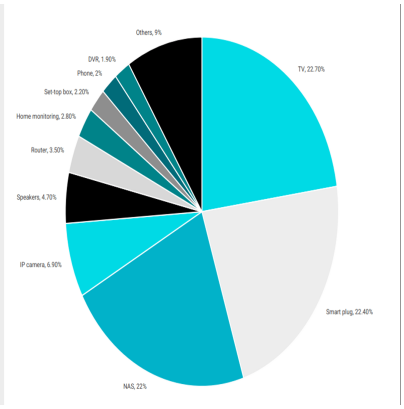


Cyberattacchi, dalle tv agli spazzolini le nostre case smart non sono mai state cosÃ¬ esposte

Descrizione

default watermark

(Adnkronos) â?? â??Se venisse fuori che alcuni dispositivi di domotica ci spiassero non mi stupireiâ?•. A dirlo allâ??Adnkronos Ã¨ Mauro Conti, professore ordinario dellâ??UniversitÃ di Padova e Ieee Fellow, esperto di cybersecurity, che commenta cosÃ¬ lâ??allarme cyber ritornato in questi giorni al centro dellâ??attenzione dopo gli attacchi alle strutture critiche, come la catena del freddo nel caso dei congelatori dei supermercati colpiti da una campagna che si inserisce in uno scenario di guerra ibrida piÃ¹ ampio e, secondo le autoritÃ , sempre piÃ¹ preoccupante. Ma mentre si parla di infrastrutture e supply chain, un altro punto di vulnerabilitÃ praticamente onnipresente sono le nostre case. Senza attenzione ad aggiornamenti e password, siamo tutti quotidianamente esposti, spiega Conti.

â??Se hai dispositivi collegati a Internet in casa, ci sono app che ti permettono di dialogare direttamente con il dispositivo, dal robottino al termostatato, dagli interruttori alle serrature, fino agli spazzolini con telecamera e ai videocitofoni: assolutamente tutti possono essere un punto di vulnerabilitÃ da cui escono dati e informazioni che i cybercriminali possono vendere onlineâ?•, spiega Conti, soprattutto se gli aggiornamenti di sicurezza di ogni dispositivo non vengono applicati, o le password aggiornate. Lâ??ecosistema domotico si Ã¨ trasformato nella piÃ¹ capillare fonte di informazioni personali mai vista. Oggigiorno, una casa media possiede 24 dispositivi connessi, secondo una ricerca di ottobre di Bitdefender e Netgear. La catena che lega la nostra voce alla lampadina del salotto Ã¨ piena di anelli deboli, presi di mira da oltre 820.000 attacchi informatici al giorno a livello globale (circa 1.000 ogni 105 secondi, secondo le stime di SentinelOne e Dexpose).

Con lâ??Internet of Things i sensori che ci espongono hanno varcato la porta dâ??ingresso. Alla quale intanto il resto di Internet bussa in continuazione: programmi automatizzati che controllano milioni di abitazioni alla ricerca di un bersaglio facile, come un dispositivo che utilizza ancora la password originale. Il secondo metodo piÃ¹ comune di attacco (dopo il port scanning, il semplice rilevamento di porte aperte in una rete) Ã¨ indovinare le password, con 466,6 milioni di tentativi registrati, su 10 milioni e mezzo di case analizzate nella ricerca Bitdefender.

Nella stessa ricerca Ã¨ emerso che il 99% delle vulnerabilitÃ erano conosciute e che le Smart Tv rappresentano il tipo di dispositivo piÃ¹ vulnerabile per un motivo molto semplice: sono i dispositivi che

rimangono dentro casa per piÃ¹ anni, senza essere aggiornati, e che permettono addirittura ad altri di accedere alla nostra connessione di casa per utilizzarla. Nel luglio 2026, la societÃ di sicurezza Spur ha descritto come le app gratuite per le smart tv aprono un proxy locale che viene usato per far passare sulla connessione a banda larga domestica il traffico di terze parti. E gli utenti accettano che questo avvenga al momento dellâ??installazione dellâ??app.

Al secondo posto nella classifica della vulnerabilitÃ ci sono dispositivi che dimentichiamo di avere semplicemente perchÃ© sono nascosti dentro i muri: gli interruttori intelligenti. Quando smettono di essere venduti, spesso finiscono anche gli aggiornamenti. Le famiglie conservano i dispositivi smart per 5-10 anni. La maggior parte dei produttori, tuttavia, rilascia aggiornamenti di sicurezza solo per 2-4 anni. Una vulnerabilitÃ gigantesca, paradossalmente risolvibile â??in maniera abbastanza banaleâ?•, con un aggiornamento o un cambio password, spiega Conti.

Ci si circonda sempre piÃ¹ di strumenti connessi, utili a ottimizzare e gestire la vita quotidiana, gli impianti industriali e i servizi, senza valutare fino in fondo il rischio che possano essere abusati da un attore malevolo, spiega Conti. Il problema principale dei dispositivi connessi non Ã¨ lâ??utilitÃ della tecnologia, ma la sua mancata protezione. Nel caso dei congelatori collegati a Internet, la possibilitÃ di gestire da remoto manutenzione, controllo e persino operazioni come lo scongelamento puÃ² rappresentare un vantaggio operativo ed economico, ma diventa un rischio se gli accessi non sono adeguatamente protetti. Un episodio su larga scala come lâ??attacco ai frigoriferi europei produce conseguenze perchÃ© â??ha un impatto non solo in una singola azienda, ma anche sulla catena di distribuzioneâ?•. Per questo motivo, vedere supermercati in diverse cittÃ e Paesi colpiti dallo stesso problema suscita â??unâ??attenzione enormeâ?•. Ma anche in quel caso, come in quello dello sfruttamento delle vulnerabilitÃ di casa, â??chiunque puÃ² essere lâ??autoreâ?•: non servono risorse economiche o tecniche particolarmente elevate. â??Attualmente ci sono strumenti di intelligenza artificiale che danno un enorme supporto da questo punto di vistaâ?•, afferma Conti.

default watermark

â??

economia

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 10, 2026
Autore
redazione