Telecamere di sicurezza, ecco perché possono essere a rischio hacker

Da tempo diversi ricercatori ed esperti si lamentano della scarsa sicurezza delle telecamere di sicurezza. Montate per lo più in bella vista per fungere da deterrente per possibili intrusioni, molte di esse vengono invece sfruttate come armi di offesa da parte degli hacker. Secondo *Fortune.com*, l'ultima moda in fatto di attacchi hacker, basata sulla vulnerabilità che consente ai malintenzionati di depistare il traffico di centinaia di migliaia di telecamere tramite attacchi Ddos, che molto semplicemente metto ko le telecamere che finiscono offline finché non viene pagato un riscatto.

Un allarme sicurezza sul rischio di attacchi massivi a telecamere di sicurezza è stato lanciato mercoledì scorso da Akamai.

Un nuovo obiettivo dei criminali sono anche le telecamere a circuito chiuso, utilizzate soprattutto in ambito televisivo. I modelli vulnerabili secondo gli esperti di Akamai sono prodotti dalle cinesi Hikvision e Dahua e dalla brasiliana Intelbras.

Quando questi dispositivi disegnati per restare su una Lan finiscono online sulla rete Internet pubblica, gli hacker sono in grado di ridirigere il traffico e bloccarne il funzionamento anche perché l'azionamento a distanza non è previsto.

Che fare per proteggere i device? Forse, prosegue Fortune, la cosa migliore sarebbe che i produttori munissero i dispositivi

di strumenti di aggiornamento automatico, per la realizzazione di patch. Una eventualità non certo dietro l’angolo e che comunque non risolvere il problema alla radice, vista la quantità di telecamere installate che ci sono in giro.

> *Telecamere di sicurezza, ecco perché possono essere a rischio hacker*