Da: Massimiliano.Troilo <> mercoledì 28 aprile 2021 10:29
Inviato: [CG] Redazione Report
A: Marco.Borsoi
Cc: incontro del 23 Aprile
Oggetto:

Categorie:

Egregio Dott. Valesini,
faccio seguito al nostro incontro per meglio circostanziare la situazione relativa a quanto avete riscontrato in Rai, in relazione alle "chiamate" fatte dalle telecamere ad un server esterno.
Prima di tutto ci rendiamo disponibili ad affiancare i vostri esperti che hanno testato i prodotti, per garantire la massima qualità delle informazioni e tutto il supporto per dimostrare che i gli stessi sono conformi alle aspettative di sicurezza e riservatezza di cui tutti gli utenti devono essere garantiti.
Come dicevo nel colloquio è difficile rispondere a domande molto tecniche se non si hanno tutti i contorni ben definiti come: il prodotto specifico oggetto del test, il firmware a bordo e, cosa più importante, i parametri di programmazione.
Come Le dicevo i prodotti sono fatti per soddisfare molteplici usi, dal residenziale o piccolo commerciale dove l'utente interagisce autonomamente con il sistema tramite il cloud, ovviamente protetto da protocolli di sicurezza e password, sino ai sistemi più complessi dove c'è la necessità, oltre alla cura delle caratteristiche di cybersecurity del device stesso, anche e maggiormente di avere una infrastruttura di rete sicura e possibilmente chiusa.

In relazione alle diverse tipologie chi installa e programma il device deve avere cura di agire sulla programmazione ed adattare il comportamento del device al reale utilizzo, pertanto penso che le "chiamate" che avete riscontrato siano attribuibili al fatto che sia stata lasciata nella programmazione la configurazione del tipo "cloud", che quindi il device continui a cercare generando le "chiamate" riscontrate, rispetto a quella che avrebbe dovuto essere una programmazione per uso locale che non prevede nessuna "chiamata".
Tecnicamente è un po' complesso da spiegare perché entrano in gioco diversi parametri quali le caratteristiche di rete, che possono andare da IP dinamici (e che quindi potrebbero aver bisogno del Cloud o del servizio DNS come punto di "incontro" per la consultazione dell'utente) a IP statici o reti indipendenti completamente chiuse che non hanno nessuna esigenza del cloud perché in comunicazione diretta.

Preciso inoltre.
Hikvision, in quanto leader di mercato all'interno del settore della sicurezza, è costantemente impegnata a garantire i più alti standard qualitativi di cybersecurity e non solo, relativamente a quanto concerne l'ambito produttivo di telecamere e videoregistratori.
Avente ruolo di produttore, in Italia Hikvision non commercializza direttamente i propri prodotti verso gli Utilizzatori Finali e pertanto non supervisioniamo in alcun modo l'operatività dei nostri
prodotti, una volta consegnati al mercato. Ad ogni modo, assicuriamo che le nostre telecamere sono progettate e prodotte osservando i più alti standard di sicurezza Cyber, per assicurare la privacy e proteggere la sicurezza pubblica.

Hikvision dedica significativi investimenti alla resilienza cyber dei suoi prodotti, implementando inoltre le seguenti iniziative:

- Hikvision produce tutti i prodotti con l'imperativo del **"Secure-by-Desing" e "Secure-by-Default"**. La cybersecurity è quindi automaticamente incorporata nei prodotti
- Tutte le componenti software di Terze Parti, eventualmente impiegate nei nostri prodotti, sono estensivamente testate dal **Product Security Team**, gruppo dedicato alle attività di analisi e basato presso i nostri HQ, prima di essere implementate;
- La gestione delle vulnerabilità (Vulnerability Management) dei prodotti è essenziale nel nostro settore. Hikvision ha designato uno specializzato team dedicato alla gestione e all'intervento in materia di sicurezza informatica (Hikvision Security Response Team) ed è stata **accreditata come CVE Numbering Authority (CNA)** dall'entità Mitre.org, ente privato noprofit che da decenni si propone come consulente impegnato nella guida tecnica e di engineering per le principali agenzie federali statunitensi anche tramite l'FFRDC (Federally Funded Research and Development Centers);
- Allo stato attuale, Hikvision è ancora la sola azienda al Mondo, fra quelle operanti nel settore della sicurezza, che si è dotata di un Source Code Transparency Center (SCTC), situato in California, dove viene dato accesso, senza restrizioni, a rappresentanti di enti governativi, per la valutazione dei codici sorgenti dei nostri prodotti.

Saluti/Best Regards/祝商祺

Massimiliano Troilo/麦克斯
Hikvision Italy BU President

***HIKVISION Italy* S.r.l.**

Vittorio Veneto | **Roma** | **Milano** | **Bologna** | **Napoli** | **Bari**