HIKVISION®

VITTIME DELLA RETE

Come proteggere l'intero
sistema di videosorveglianza
dalle insidie della rete (e da occhi indiscreti)

HIKVISION®

SOMMARIO

Come proteggere l'intero sistema di videosorveglianza dalle insidie della rete (e da occhi indiscreti)

Caro lettore,

ti invitiamo a leggere con estrema attenzione questa guida poiché contiene informazioni determinanti per la sicurezza dei dispositivi che utilizzi o che installi. Parleremo principalmente dei sistemi di videosorveglianza, ma tieni bene a mente che tutti i consigli contenuti nella sezione reti ti aiuteranno a proteggere la tua privacy ogni volta che sarei connesso.

Tutti i dispositivi IoT, come personal computer, smartphone, smart speaker, play station, ecc., possono infatti rappresentare un pericolo quando connessi ad una rete poiché questa funge da veicolo per le informazioni memorizzate, trasmesse o elaborate dal tuo dispositivo. Se non adeguatamente protetta, dunque, la rete espone i tuoi dati rendendoli vulnerabili e accessibili a chiunque, anche quando il dispositivo che utilizzi possiede elevati standard di sicurezza.

Non è quindi il marchio, il produttore o un dispositivo specifico a rappresentare un pericolo per la tua privacy, ci sono altri fattori imprescindibili da tenere in considerazione, primo tra tutti la rete. A seguire, occorre accertarsi che il dispositivo supporti protocolli sicuri, sia adeguatamente configurato e venga aggiornato ad ogni nuova versione disponibile.

Ci auguriamo che questa piccola premessa ti guidi in una lettura imparziale del documento, immune quindi a qualsiasi parere personale o forzatamente inculcato dai mass media, il cui unico interesse è aumentare l'audience a costo di diffondere notizie errate, fuorvianti e perfino manomesse (che per quanto ci riguarda smentiremo nelle ultime pagine del report).

“Il potere dei mezzi di comunicazione di massa risiede nella capacità di modellare una determinata realtà sociale. Gli spettatori, anche i meno attenti, in qualche misura sono investiti da questo potere, trasferiscono le informazioni mediatiche nella percezione del loro mondo reale (Bandura, 2001). Secondo la Teoria della Coltivazione (Gerbner, Gross, Morgan, Signorielli, & Shanahan, 2002), i mezzi di comunicazione tendono a sovra-rappresentare alcuni fenomeni sociali rispetto alla loro reale incidenza, operando in questo modo una distorsione della realtà. Un’elevata esposizione a tali distorsioni mediatiche si traduce nella percezione che il fenomeno sovra-rappresentato rifletta la realtà del mondo che ci circonda.”

In un mondo in cui ognuno agisce per i propri interessi, puoi fare affidamento su una cosa soltanto: la tua mente. Lascia che sia lei a condurti verso l’oggettività dei fatti attraverso l’analisi di dati e considerazioni inconfutabili.

Le parole possono influenzare tanto e a lungo, ma l’unica cosa che tornerà a galla in un mare di informazioni contrastanti sarà solo la verità.

Buona lettura
Hikvision Italy

MASSIMILIANO TROILO
GENERAL MANAGER HIKVISION ITALIA

Cosa dice il Regolamento Europeo per la Protezione dei Dati?

Le Linee Guida sottolineano come il titolare dovrebbe adottare idonee misure tecniche e organizzative che consentano di mantenere costantemente il controllo degli strumenti impiegati (infrastruttura hardware e software del sistema di monitoraggio) e garantiscano integrità, disponibilità e riservatezza dei dati in ogni fase del trattamento (memorizzazione, trasmissione ed elaborazione).

Come stabilito dall'art. 25 GDPR, i titolari dovrebbero scegliere tecnologie in grado di difendere la privacy, ad esempio, sistemi che possono essere configurati in modo da consentire al titolare di oscurare o sfocare parti del video che riprendono anche soggetti diversi dall'interessato, onde permettere loro di esercitare i diritti ex art. 15 e ss.

Un sistema di videosorveglianza è costituito da dispositivi analogici e digitali e da un software che permette di catturare le immagini di una scena, gestirle e mostrarle all'operatore preposto (es. il titolare del trattamento). I suoi componenti sono raggruppati nelle seguenti categorie:

1) **ambiente video**: acquisizione delle immagini, interconnessioni e gestione delle immagini. Lo scopo della cattura delle immagini è la generazione di un'immagine del mondo reale in un formato tale da poter essere utilizzata dal sistema di videosorveglianza;

2) **le interconnessioni** descrivono tutte le trasmissioni di dati all'interno dell'ambiente video (connessioni e comunicazioni). Esempi di connessioni sono i cavi, le connessioni digitali e le trasmissioni wireless. Le comunicazioni descrivono tutti i segnali video e di controllo dei dati, che possono essere digitali o analogici;

3) **la gestione delle immagini** include l'analisi, la memorizzazione e la presentazione di un'immagine o di una sequenza di immagini;

Dal punto di vista della gestione del sistema, un sistema di videosorveglianza possiede le seguenti funzioni logiche:

1) **data management e activity management**, che comprendono la gestione dei comandi dell'operatore e delle attività generate dal sistema (procedure di allarme, avviso degli operatori);
2) **le interfacce con altri sistemi** possono includere il collegamento ad altri sistemi di sicurezza (controllo accessi, allarme antincendio) e di altri sistemi che non riguardano la sicurezza (sistemi di gestione degli edifici, riconoscimento automatico delle targhe);
3) **la sicurezza di un sistema di videosorveglianza** consiste nella riservatezza, nell'integrità e nella disponibilità;
4) **la sicurezza del sistema** include la sicurezza fisica di tutti i componenti del sistema e il controllo degli accessi al sistema di videosorveglianza;
5) **la sicurezza dei dati** comprende la prevenzione della perdita dei dati, ovvero la loro manipolazione.

Data protection by design e by default

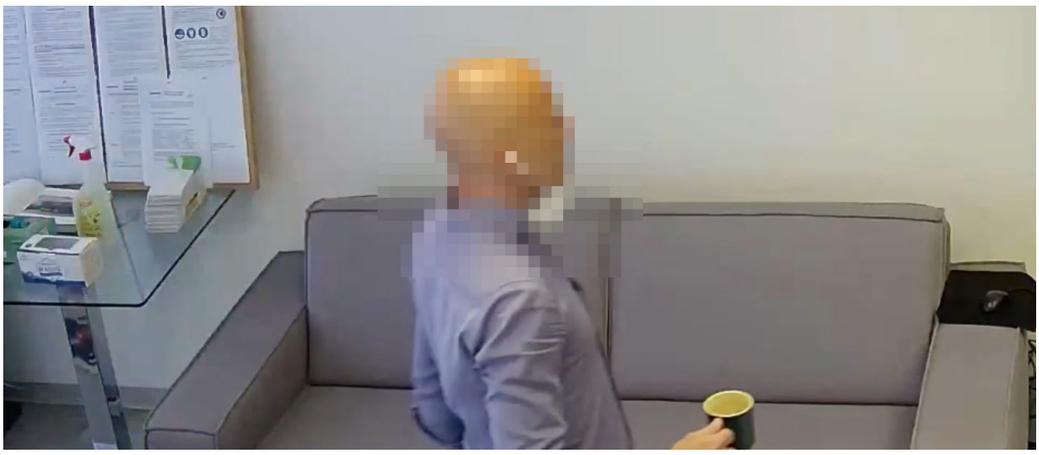
Come stabilito dall'Art. 25 del GDPR, i titolari del trattamento devono attuare misure tecniche e organizzative adeguate in materia di protezione dei dati prima dell'installazione di un sistema di videosorveglianza (by design), ossia prima di iniziare la raccolta e l'elaborazione dei dati mediante le telecamere, utilizzando per impostazione predefinita i soli dati necessari per le finalità del trattamento (by default).

Tali principi sottolineano la necessità di avvalersi di tecnologie integrate per il miglioramento della protezione dei dati, di **impostazioni predefinite che riducano al minimo il trattamento dei dati**, nonché di strumenti necessari per garantire la massima protezione possibile ai dati personali.

I titolari del trattamento dovrebbero integrare la protezione dei dati anche da un punto di vista organizzativo. In questo caso il titolare del trattamento dovrebbe adottare un quadro di gestione adeguato, nonché definire e applicare le policy e le procedure relative alla videosorveglianza.

Come stabilito dall'articolo 25 del RGPD, i titolari del trattamento devono mettere in atto adeguate misure tecniche e organizzative di protezione dei dati non appena pianificano l'installazione di un sistema di videosorveglianza, prima di iniziare la raccolta e il trattamento di filmati.

Questi principi sottolineano la necessità di tecnologie integrate per il miglioramento della privacy, impostazioni predefinite che riducano al minimo il trattamento dei dati e l'adozione degli strumenti necessari ai fini della massima protezione possibile dei dati personali.



Esempi di questo tipo di tecnologie sono i sistemi che consentono il mascheramento o l'offuscamento delle zone irrilevanti per la sorveglianza, oppure l'editing di immagini di terzi, quando si forniscono filmati agli interessati. D'altra parte, le soluzioni individuate non dovrebbero prevedere funzioni non necessarie. **Le funzioni fornite, ma non necessarie, devono essere disattivate**.

La maggior parte delle misure che possono essere utilizzate per la sicurezza dei trattamenti di videosorveglianza, soprattutto quando si utilizzano apparecchiature digitali e software, sono sostanzialmente identiche alle **misure utilizzate in altri sistemi informatici**. Tuttavia, indipendentemente dalla soluzione prescelta, il titolare del trattamento deve proteggere adeguatamente tutti i componenti di un sistema di videosorveglianza e i dati in tutte le fasi, vale a dire durante la conser-

vazione (dati a riposo), la trasmissione (dati in transito) e il trattamento (dati in uso).

La sicurezza del sistema e dei dati può comprendere:

1) **protezione dell'intera infrastruttura del VSS** (comprese telecamere remote, cablaggio e alimentazione) contro manomissioni fisiche e furti;

2) **protezione della trasmissione di filmati** attraverso canali di comunicazione sicuri a prova di intercettazione;

3) **cifratura dei dati**;

4) **utilizzo di soluzioni basate su hardware e software quali firewall**, antivirus o sistemi di rilevamento delle intrusioni contro gli attacchi informatici;

5) **rilevamento di guasti** di componenti, software e interconnessioni;

6) **strumenti per ripristinare la disponibilità** dei dati personali e l'accesso agli stessi in caso di problemi fisici o tecnici.

Le misure che supportano il controllo fisico e logico degli accessi includono:

1) **l'attuazione** di metodi e mezzi di autenticazione e autorizzazione dell'utente, tra cui ad esempio la lunghezza delle password e la **frequenza della loro modifica**;

2) **la registrazione** e la **revisione periodica delle azioni eseguite** dagli utenti (con riguardo sia al sistema sia ai dati);

3) **l'esecuzione** del **monitoraggio e l'individuazione di guasti agli accessi in modo continuativo** e la risoluzione in tempi brevi delle carenze individuate.

Attuare queste misure tecniche e organizzative è fondamentale perché quando c'è di mezzo la rete nessun dispositivo è 100% sicuro, se la rete stessa non è sicura.

L'unica soluzione è quindi una e una soltanto: assicurarsi una rete privata, sicura e davvero blindata.

L'installatore, per raggiungere questo obiettivo, deve necessariamente essere un esperto di reti o collaborare con questa figura per garantire la messa in sicurezza della rete. Durante gli accessi da remoto deve inoltre evitare categoricamente l'utilizzo di soluzioni "di fortuna" come software gratuiti e liberi per il collegamento remoto, che purtroppo vengono spesso utilizzati in assenza di competenze specifiche.

Ecco di seguito le principali accortezze per una rete sicura

1. Scegliere una password sicura

La prima cosa da fare è impostare una buona password per proteggere l'accesso alla propria rete. Per essere considerata sicura, una password deve rispondere ad alcuni importanti requisiti:

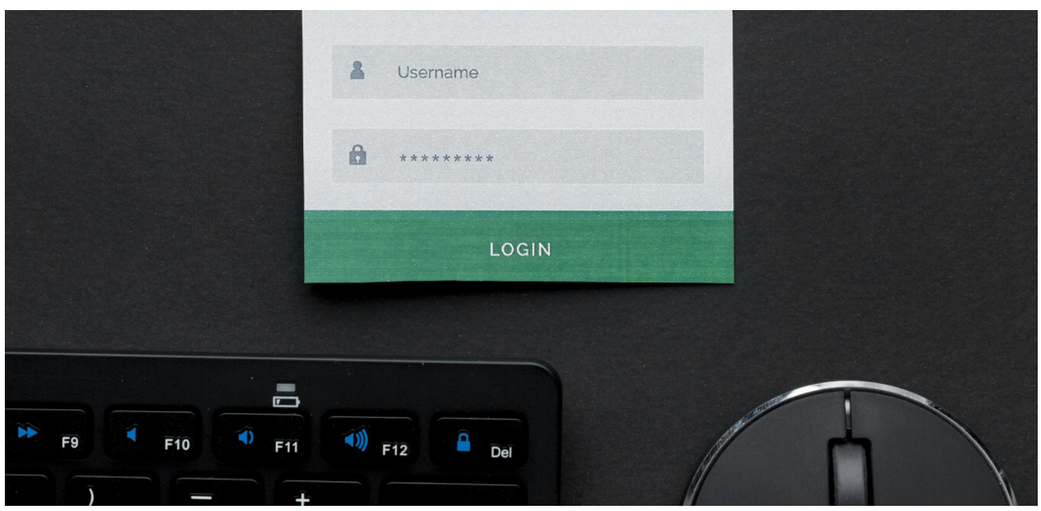
- Non deve essere stata mai utilizzata in passato né essere in uso per altri servizi.
- Non deve essere facilmente riconducibile all'utente, quindi vanno evitate date di nascita, nomi di parenti, ecc.

- Deve essere lunga almeno 10 caratteri e contenere lettere maiuscole e minuscole, numeri e caratteri speciali.
- Non deve mai essere salvata e compilata in automatico.

Curiosità

Esistono degli algoritmi di machine learning in grado di sviluppare password incrociando i dati degli utenti e le password maggiormente utilizzate. Pensiamo ad esempio alla combinazione “nome + data di nascita”, che sia nostra o dei nostri figli, oppure alla data del nostro anniversario. Quanti di noi, almeno una volta, li hanno utilizzati per creare una password?

Se vuoi che nessuno risalga alla tua password, sia esso una macchina o un essere umano, fai in modo che rispetti quanto detto in precedenza e presta attenzione ai plug in o alle estensioni che installi sui browser web. Si tratta spesso di applicazioni gratuite, e un prodotto non è mai gratuito: il prezzo da pagare, in questo caso, sono i nostri dati (e le nostre password!).



2. Modificare le impostazioni predefinite del router

Per accedere alle impostazioni del router è necessario usare nome utente e password forniti dal produttore dell’hardware. Non molti sanno però che questi dati in alcuni casi sono uguali per tutti gli utenti, e quindi sostanzialmente pubblici. È consigliabile impostare delle credenziali di accesso personalizzate, in modo che nessun altro possa accedere al proprio pannello di controllo.

Se il router lo permette, è anche consigliabile disabilitare la sua gestione remota, cioè da un computer collegato a una rete diversa. Così facendo, sarà possibile accedere al pannello di controllo, e quindi modificare le impostazioni, soltanto una volta già collegati alla rete stessa.

Anche in questo caso, scegli con cura le credenziali da utilizzare.

3. Aggiornare il firmware del router

A volte i router presentano delle vulnerabilità particolari che possono essere sfruttate per ottenere l'accesso a una rete privata. I produttori di questo tipo di dispositivi sono però solitamente molto rapidi nel porre rimedio a queste vulnerabilità, rilasciando frequentemente aggiornamenti firmware.

È perciò importante verificare regolarmente che il firmware installato sia aggiornato alla versione più recente disponibile.

4. Abilitare il firewall del router

Un firewall è un metodo di difesa che filtra il traffico di rete bloccando le comunicazioni ritenute poco sicure. Molti sistemi operativi mettono a disposizione un firewall predefinito, come ad esempio Windows Defender, ma è possibile anche installarne di diversi.

Nei router è poi solitamente presente un ulteriore firewall che protegge tutti i dispositivi collegati. È importante quindi assicurarsi che sia attivato e configurato in modo da garantire la massima protezione. Spesso, infatti, è possibile scegliere il tipo di protezione che si desidera, ma l'impostazione predefinita garantisce soltanto una sicurezza media.

5. Nascondere la rete WiFi

Ogni rete WiFi deve essere definita da un nome, o meglio da un SSID (Service Set Identifier). Un primo e fondamentale consiglio è di evitare di usare il nome predefinito impostato dal produttore, ma ancora più sicuro è nascondere del tutto la rete.

Dopo aver configurato tutti i dispositivi e aver controllato che si possano collegare in modalità wireless senza problemi, è quindi consigliabile accedere alle impostazioni dell'access point e disabilitare la trasmissio-

ne dell'SSID, a volte chiamata anche SSID broadcast. In questo modo la rete WiFi non sarà più visibile nelle ricerche, rendendo più difficili eventuali attacchi esterni.

Alcuni router in commercio permettono di creare una vera e propria lista di dispositivi abilitati a connettersi alla rete, in base al MAC address del dispositivo che si vuole agganciare alla rete WiFi. Qualsiasi altro dispositivo e di qualsiasi natura non potrà in alcun modo connettersi e quindi entrare nella nostra rete.

6. Abilitare il filtro MAC

Per migliorare ancora di più la sicurezza della propria rete WiFi, è possibile anche autorizzare l'accesso soltanto ad alcuni dispositivi sfruttando il filtro MAC, o MAC filtering, messo a disposizione dai router.

Ogni dispositivo abilitato alla connessione di rete è identificato da un codice alfanumerico univoco chiamato indirizzo MAC: solitamente lo si può ricavare dalle impostazioni del dispositivo stesso o dal manuale di istruzioni. Questo codice va inserito nella pagina relativa al filtro MAC del pannello di controllo del router.

Le informazioni che transitano, ad esempio, tra una telecamera ed un videoregistratore vengono trasmesse attraverso un frame che contiene l'indirizzo della scheda rete mittente e quello della scheda rete destinatario. Ipotizziamo che il mittente sia il videoregistratore. Grazie al protocollo ARP (Address Resolution Protocol), il cui compito è fornire la "mappatura" tra l'indirizzo IP e l'indirizzo MAC corrispondente di un terminale in una rete locale ethernet, il videoregistratore può comunicare con una telecamera specifica (quindi caratterizzata da un determinato indirizzo IP e un MAC Address).

È possibile abilitare il Dynamic Host Configuration Protocol (protocollo applicativo che permette ai dispositivi di una certa rete locale di ricevere automaticamente ad ogni richiesta di accesso) solo con certi MAC Address prestabiliti.

Così facendo viene impedito l'accesso alla rete da parte di dispositivi il cui indirizzo MAC non è compreso nell'elenco.

Curiosità

Un possibile attacco è il MAC Spoofing: un dispositivo malevolo sulla rete invia un pacchetto ARP ad un altro dispositivo modificando l'abbinamento MAC-IP. In questo modo il dispositivo attaccato invierà i dati ad una scheda di rete destinataria diversa da quella corretta. In questo modo è possibile impossessarsi di un indirizzo IP già presente sulla rete.

Consigli

Anche in questo caso, utilizzando apparati professionali è possibile abilitare delle funzioni di protezione contro questo tipo di attacchi (ad esempio negando l'accesso a dispositivi sconosciuti, o permettendo la connessione solo a MAC address presenti in una lista).

7. Utilizzare una VPN

Una VPN è una rete virtuale privata che si interpone tra i dispositivi all'interno della rete e che permette di creare un "tunnel" sicuro anche quando la connessione avviene tramite rete pubblica. All'interno di questo tunnel i dispositivi della tua rete, come la telecamera e il videoregistratore, possono scambiarsi informazioni sottoforma di pacchetti crittografati invisibili a terze parti e quindi a tutto ciò che passa al di fuori del tunnel.

Nel data center dell'azienda, o nel suo private cloud (nel caso si abbia optato per questa soluzione), deve essere installato un server VPN su cui sono gestiti tutti e tre i livelli del framework di sicurezza di una Virtual Private Network:

- un sistema di autenticazione degli utenti;
- un layer per la gestione dei metodi di cifratura dei dati scambiati fra i vari nodi della rete;
- un firewall che controlla gli accessi alle diverse porte delle reti.

8. Utilizzare una VLAN

Per aumentare ulteriormente la sicurezza della rete è consigliato crea-

re e configurare una VLAN, ovvero una rete di area locale virtuale. È un tipo di LAN, il nome che viene dato alle reti locali utilizzate per abitazioni e aziende, ma virtuale.

Semplificando molto il concetto, una VLAN è una rete fittizia di dispositivi che sono connessi su varie porte di apparati diversi (switch e access point, per esempio) e vengono connessi virtualmente ad una LAN. Una VLAN serve a:

- Suddividere i dispositivi collegati a una rete in base a certe caratteristiche
- Collegare dispositivi separati

Esistono due grandi tipologie di VLAN: basate su porte e basate su tag.

Nelle VLAN basate su porte, ogni porta è associata a una sottorete e il traffico viene smistato dallo switch in funzione delle porte. Nel secondo caso, VLAN basate su tag, si aggiunge un tag ai pacchetti di dati (frame ethernet) con le informazioni della VLAN, in particolare il cosiddetto VID (identificatore VLAN). La scelta tra questi due tipi di rete dipende dalle necessità degli utenti.

9. Disabilitare l'UPnP e altre funzionalità non necessarie

Una funzionalità spesso abilitata di default nei router è l'UPnP, un protocollo che permette di rendere più semplice la connessione diretta tra dispositivi e host remoti. Si tratta di un'opzione che può essere molto utile ma allo stesso tempo molto pericolosa. L'UPnP può infatti essere sfruttato per aprire istantaneamente le porte sul router per far raggiungere i dispositivi della rete privata via internet su ip pubblico. Un'altra funzionalità che, a meno di esigenze particolari, può essere disattivata (o limitata) è il DHCP, cioè il protocollo che assegna automaticamente un indirizzo IP a ogni dispositivo connesso alla rete. È infatti preferibile assegnare manualmente gli indirizzi IP, in modo da averne sempre il pieno controllo. Entrambe le funzionalità possono essere disabilitate nelle impostazioni del router e riattivate in caso di necessità. In alcuni router è possibile assegnare l'indirizzo IP in maniera dinamica solo ai dispositivi "conosciuti", ovvero dispositivi il cui MAC Address è già noto e inserito in apposita lista.

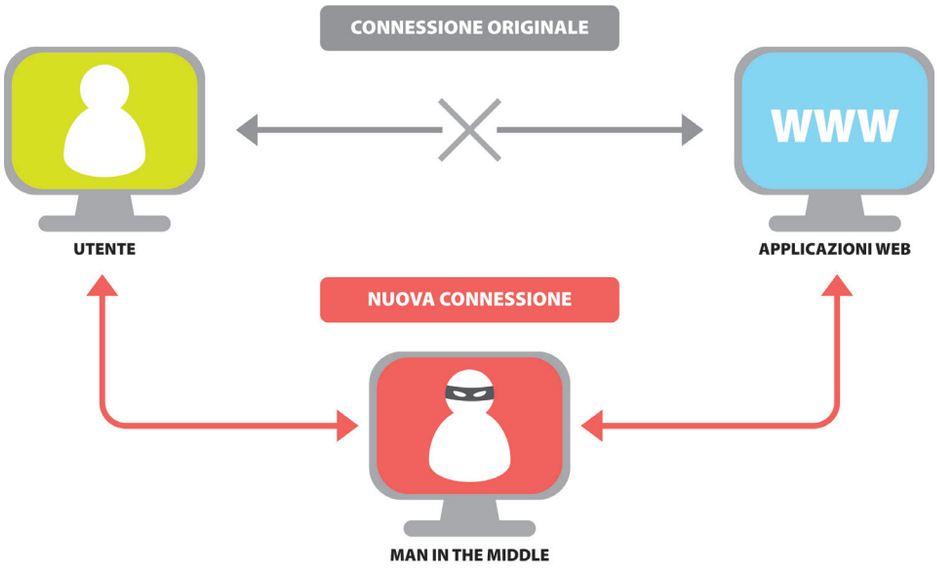
Curiosità

Un tipo di attacco è il DHCP Spoofing: la presenza di un dispositivo

malevolo sulla rete attiva un secondo DHCP Server che assegna parametri di rete ai dispositivi che lo richiedono, facendo transitare i dati dei client attraverso di esso e riuscendo in questo modo a leggere il contenuto dei pacchetti trasmessi (Man in the middle).

Consigli

I router e switch professionali, solitamente, permettono di indicare su quale porta è presente il DHCP Server (Trusted Port). Se su una porta non assegnata (Untrusted port) viene attivato un DHCP Server malevolo, i suoi pacchetti non vengono trasmessi.



Dopo aver garantito la sicurezza della rete si passa al dispositivo

Qualsiasi dispositivo connesso alla rete, durante la fase di configurazione, deve essere “pulito” di tutte quelle funzioni abilitate di default che potrebbero mettere a rischio l’intero sistema. L’esempio più banale è quello della geolocalizzazione sul nostro telefono. Se attivata permette infatti a tutte le app autorizzate di conoscere la nostra posizione in tempo reale. Se disattivata, invece, non rappresenta un pericolo e ci limita solo in alcune funzioni, come ad esempio il navigatore.

Lo stesso discorso vale per qualunque altro dispositivo connesso alla rete, anche il più semplice, che può disporre di funzionalità base come l’impostazione automatica di data e ora, il meteo, ed altro. Disattivate le funzioni che richiedono, per forza di cose, la comunicazione con l’esterno, i singoli dispositivi e l’intero sistema cesseranno di trasferire

dati all'esterno.

Così come definito anche nelle linee guida del EDPB – "le funzioni fornite ma non necessarie devono essere disattivate".

Occorre inoltre assicurarsi che il dispositivo in questione supporti protocolli sicuri e venga aggiornato correttamente ad ogni nuovo firmware disponibile. L'aggiornamento può essere automatico o, per una maggiore sicurezza, manuale, ma rimane responsabilità dell'utilizzatore del sistema.

NOTA: sottolineiamo nuovamente l'importanza di dotarsi di versioni firmware aggiornate e create appositamente per sconfiggere le vulnerabilità riscontrate nelle versioni precedenti.

Il contro-esperimento condotto sulle telecamere Hikvision in presenza di una rete sicura, firmware aggiornati e funzioni secondarie disabilitate ha smentito l'esito della simulazione condotta durante la trasmissione Report confermando la validità del dispositivo e delle misure precauzionali consigliate.

Effettuato con lo scopo di rispondere alle richieste dei nostri clienti a seguito della trasmissione, questo esperimento è stato descritto all'interno di un documento tecnico che dimostra la sicurezza dei dispositivi Hikvision ed elenca tutti i protocolli e standard crittografici impiegati per garantire la sicurezza dei dati.

Riportiamo di seguito quanto contenuto all'interno del documento.

Hikvision, contestualizzazione ed informazioni sulla sicurezza

Hikvision Italy Srl è una realtà italiana, composta da personale italiano, che rispetta le leggi e regolamentazioni in vigore sul territorio italiano e, in generale, nell'area UE.

Hikvision Italy Srl, rispetto agli Head Quarters situati in Cina, costituisce una stabile organizzazione, assoggettata per legge agli obblighi societari italiani in materia ovviamente di fiscalità e contabilità, ma anche in materia contrattualistica e soprattutto di pratiche amministrative.

Hikvision Italy è stata costituita nel 2012 a dimostrazione della presa di responsabilità dell'azienda rispetto alle attività sviluppate all'interno del nostro territorio, verso operatori del settore, utenti finali e, in generale, il mercato tutto.

Hikvision conferma con forza che i propri dispositivi non inviano in nessuna occasione ed autonomamente alcun dato sensibile o immagine.

È facoltà dell'utilizzatore attivare la funzionalità per finalità intrinseche di sorveglianza, comunque consentite nel perimetro delle regolamentazioni vigenti. In tal caso, Hikvision mette a disposizione strumenti diversi per garantire la sicurezza dei summenzionati dati, quali crittografia, strumenti di trasporto sicuri sulla rete (es. HTTPS), certificati e credenziali di accesso, oltre che codici univoci di sicurezza per ogni singolo device, programmabili solo dall'utente/utilizzatore e pertanto sconosciuti ad Hikvision stessa.

Confermiamo inoltre che, contrariamente a quanto diffuso da molteplici testate giornalistiche, non vi è stata alcuna rimozione forzata delle telecamere Hikvision all'interno dei locali del Parlamento Europeo, così come non vi è alcuna procedura avviata dai funzionari di Camera e Senato per la sostituzione delle stesse.

Le fuorvianti notizie diffuse, se si legge con attenzione, fanno spesso riferimento ai termoscanner, dispositivi installati in modo massivo nell'anno 2020 per contrastare la diffusione del Covid-19. Pertanto, se in futuro tali dispositivi verranno rimossi, sarà una lieta notizia che annuncia la fine di un periodo difficile per l'umanità intera e non la rimozione di Hikvision dalla comunità Europea per ipotetiche violazioni dei

diritti umani dettate da stretti legami con l'esercito cinese.

Hikvision non ha mai condotto attività di ricerca e sviluppo per applicazioni militari cinesi e mai lo farà.

Sicurezza dei prodotti e impostazioni delle "chiamate"

Diversi sono i dispositivi che compongono il sistema di videosorveglianza, così come sono diverse le modalità di funzionamento e gli usi possibili del proprio sistema. Un prodotto deve essere dotato di tutte le funzioni richieste dal mercato per poter essere ritenuto interessante, commercializzabile ed in linea con gli standard di settore.

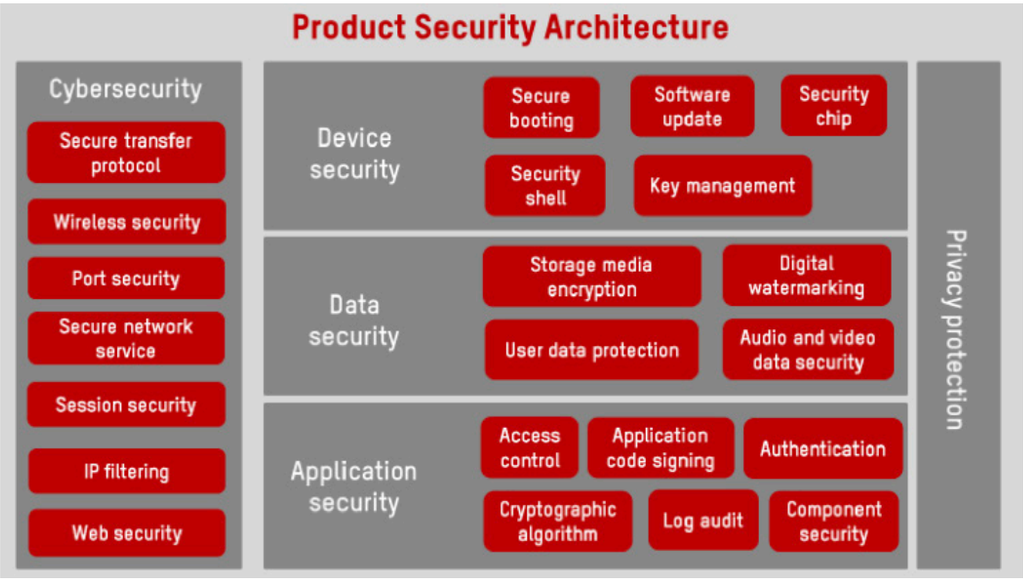
Quello che è importante è che i prodotti, pur garantendo le funzionalità di cui sopra, consentano agli operatori di attivare o disattivare le stesse a fronte dell'utilizzo desiderato, come specificato dall'European Data Protection Board.

Hikvision Italy s.r.l. ribadisce che, anche se non impostate adeguatamente dai fruitori finali, le telecamere Hikvision comunque non inviano immagini (o flussi video) a server remoti, a conferma che per Hikvision la sicurezza informatica è sempre stata (e continuerà ad esserlo) un elemento fondamentale.

In particolare, Hikvision Italy s.r.l. non offre soluzioni di tipo "Cloud storage" che prevedrebbero l'invio di flussi video ad uno storage condiviso e raggiungibile tramite una connessione ad un Cloud proprietario.

Qualora l'esigenza e l'uso lo richieda, se impostate per eseguire chiamate verso l'esterno, le telecamere e gli apparati Hikvision sono regolamentate da un programma interno di sicurezza dei prodotti che include 5 importanti aspetti:

- Sicurezza dei dispositivi
- Sicurezza dei dati
- Sicurezza delle applicazioni
- Sicurezza della rete
- Protezione della privacy



Sicurezza dei dispositivi

La sicurezza intrinseca degli apparati è implementata per assicurare che tutti i componenti di ciascun dispositivo forniscano gli adeguati livelli di sicurezza sia hardware che software. Come è pratica comune nei settori che vertono sull'elettronica e sulla connettività degli apparati, per eventuali problematiche di sicurezza che si dovessero verificare, Hikvision Italy srl rilascia periodici aggiornamenti Software disponibili per l'intera gamma prodotti.

Questa pratica è oggetto dell'attenzione del comitato interno di Cyber Security e si avvale anche delle segnalazioni che ci pervengono tramite l'adesione al CVE, ove Hikvision Italy srl è accreditata addirittura come Numbering Authority, per poter contribuire alla sicurezza generale dei prodotti e dei sistemi rivelando le vulnerabilità e rendendole conosciute alla community tutta. Nella pratica, un produttore può reagire ad una vulnerabilità scoperta solo producendo una patch e rilasciando quindi un FW (Firmware) aggiornato che la includa, non potendo operare direttamente verso gli apparati.

È con questa consapevolezza che diventa spontaneo chiedersi se i prodotti siano aggiornati e mantenuti aggiornati da parte dell'utilizzatore o di una realtà competente dall'utilizzatore incaricata.

Sicurezza dei dati

Con avanzate tecnologie crittografiche, certificate dalla FIPS con certificato 140-2, Hikvision Italy srl fornisce protezione sull'utente, sia per ciò che riguarda i dati di configurazione dell'utente che per i dati personali dell'utente. Una chiave di crittografia dei dati è creata dal generatore di codici random al primo avvio del dispositivo, permettendo una "chiave unica e univoca per ogni dispositivo".

Questo assicura che ogni dispositivo sia unico e le sue credenziali assegnate in modo randomico. Senza la chiave di un dispositivo, gli aggressori non possono decifrare alcun dato, anche se lo hanno forzatamente copiato dal dispositivo. La definizione di ogni tipo di credenziale di accesso è rimessa a chi realizza o comunque gestisce un impianto.

La protezione delle registrazioni attraverso chiave di cifratura, il Digital Watermarking e la protezione dei dati audio&video attraverso i protocolli HTTPS, DTLS e TLS si aggiungono come standard di trasmissione alle tecnologie di crittografia di sicurezza in difesa da attacchi cyber.

Sicurezza delle applicazioni

L'assenza di password di default, la generazione della stessa esclusivamente al primo avvio, il criterio di creazione complesso con caratteri alfanumerici, i diritti di accesso impostabili per singolo utente, il log audit per il monitoraggio delle attività e degli eventi (incluse anomalie e tentativi di attacco) sono tutte funzionalità che elevano il livello di protezione degli accessi ai dispositivi Hikvision Italy s.r.l. In questo, Hikvision Italy s.r.l. mette a disposizione degli utilizzatori prodotti compliant con i dettami del GDPR in relazione alla gestione delle credenziali di accesso, la loro unicità, la loro proprietà unica e i metodi ed obblighi relativi alle caratteristiche delle password stesse, alla frequenza di cambio della stessa, ecc.

Sicurezza della rete

Con l'obiettivo di garantire un elevato standard di sicurezza, Hikvision ha rimosso diversi protocolli dalle proprie telecamere e dispositivi, come Telnet, Server FTP per ridurre i tentativi di attacco. Altri protocolli di sicurezza, invece, sono disabilitati di default (SSLv3.0, TLSv1.0, SNMPv2, NTP, SSH), e abilitabili all'occorrenza e secondo le esigenze. Il protocollo Syslog supporta la trasmissione basata su TLS o DTL, e nessun dato sensibile viene divulgato.

Protezione della privacy

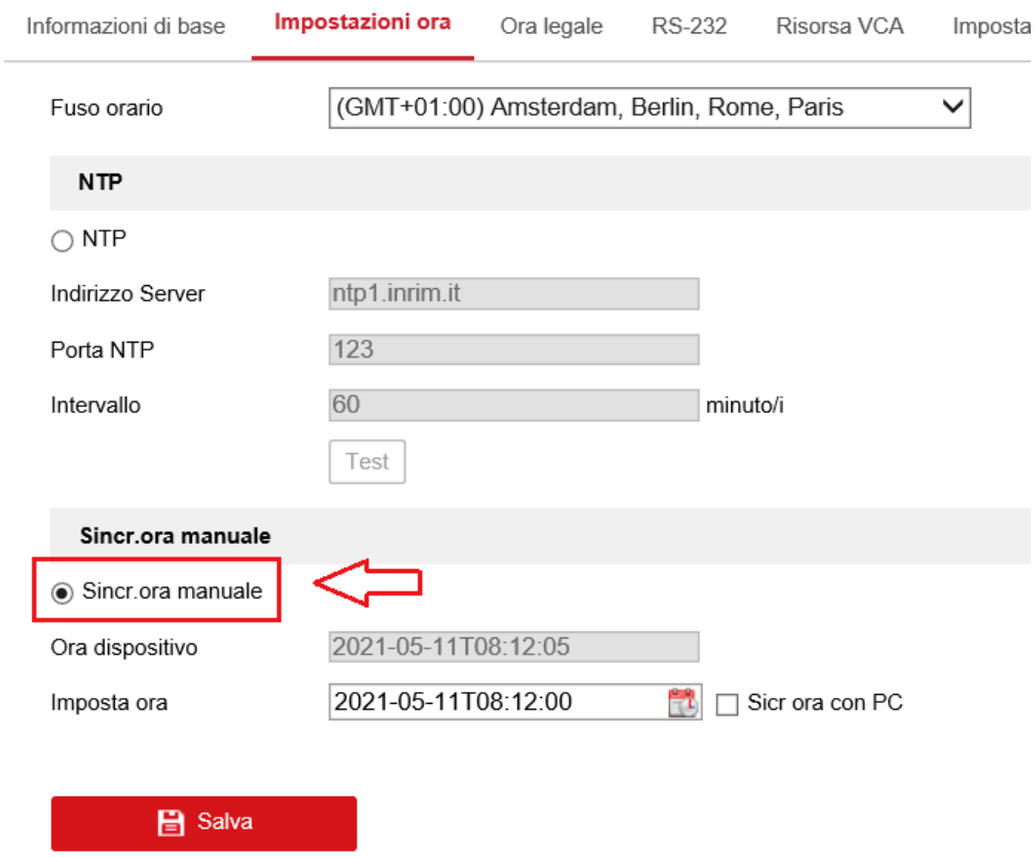
Hikvision Italy srl rispetta rigorosamente e responsabilmente le leggi e i regolamenti applicabili sulla protezione dei dati, tra cui il GDPR. Facendo riferimento alle migliori pratiche del settore, integra i concetti di sicurezza dei dati e protezione della privacy in tutto il processo aziendale completo, dallo sviluppo tecnologico, progettazione del prodotto, sviluppo, verifica, test, consegna ai servizi post-vendita.

In seguito alla puntata di Report del 10 maggio 2021, intendiamo fare chiarezza sulle "chiamate" che le telecamere eseguono verso l'esterno, in quanto alcune asserzioni dichiarate durante la trasmissione non trovano alcun riscontro nella realtà e sono state esposte come frutto di una travisazione, raggruppando diversi argomenti, anche non direttamente correlati.

A seguito di prove tecniche fatte presso i nostri laboratori, realizzate con l'impiego di software di sniffing che rilevano attività sulla rete, abbiamo riscontrato che a seconda della programmazione e dell'uso che se ne fa della telecamera, questa può generare, o meno, chiamate verso l'esterno. È assolutamente possibile, tramite semplici configurazioni dell'apparato, disabilitare ogni servizio o protocollo che preveda una comunicazione con server esterni (come dimostra l'esperimento di seguito illustrato). Ovviamente, così facendo, non saranno più disponibili determinate funzionalità. La discrezione è lasciata all'utilizzatore e al suo installatore.

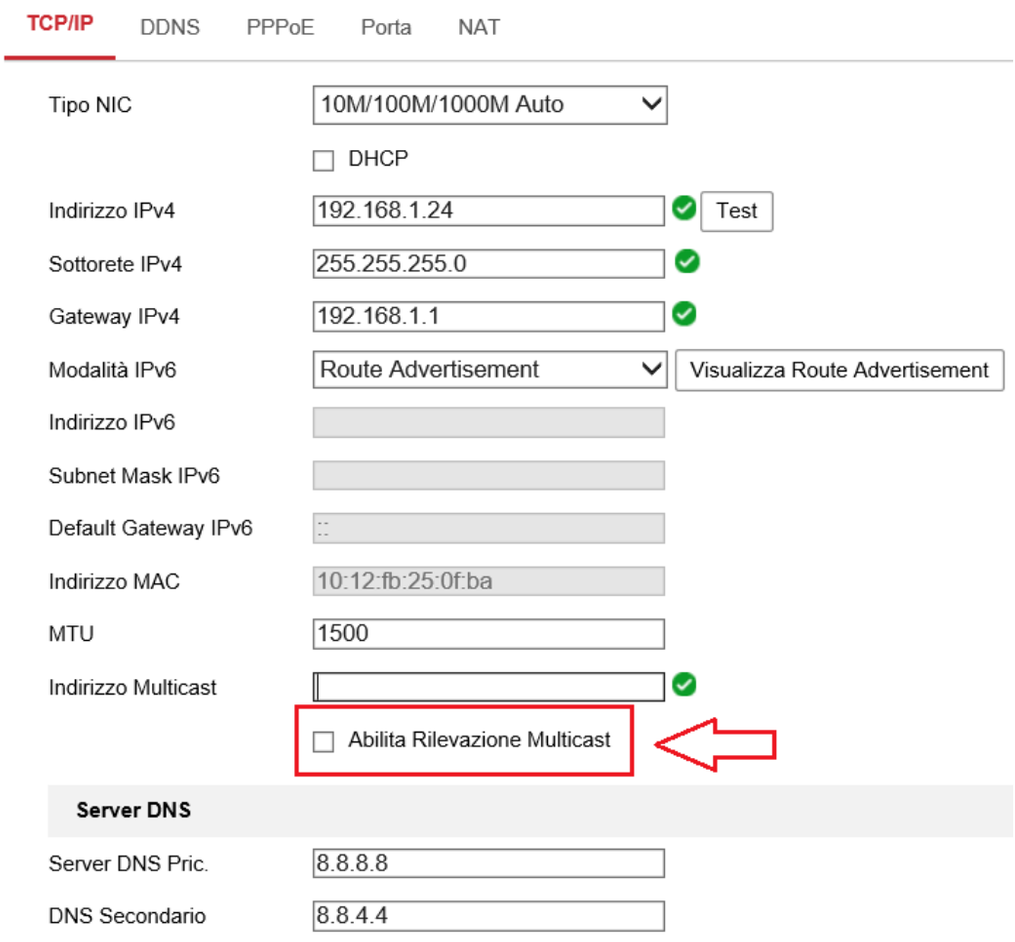
NTP SERVER (sincronizzazione dell'orario)

La configurazione dell'orario può essere affidata ad un altro apparato presente nella stessa rete della telecamera oppure alla sincronizzazione manuale (come in figura).



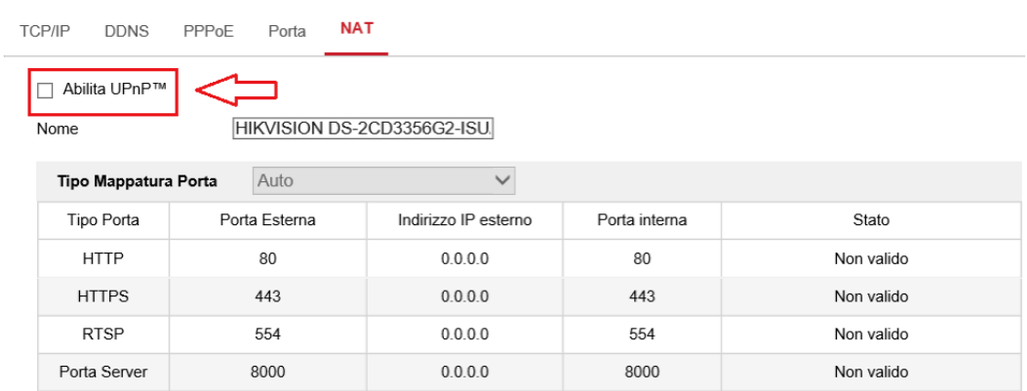
RILEVAZIONE MULTICAST (funzionalità di instradamento di più streaming in contemporanea)

A seconda di come è stato predisposto il sistema di videosorveglianza, questa funzione può rimanere disabilitata o meno.



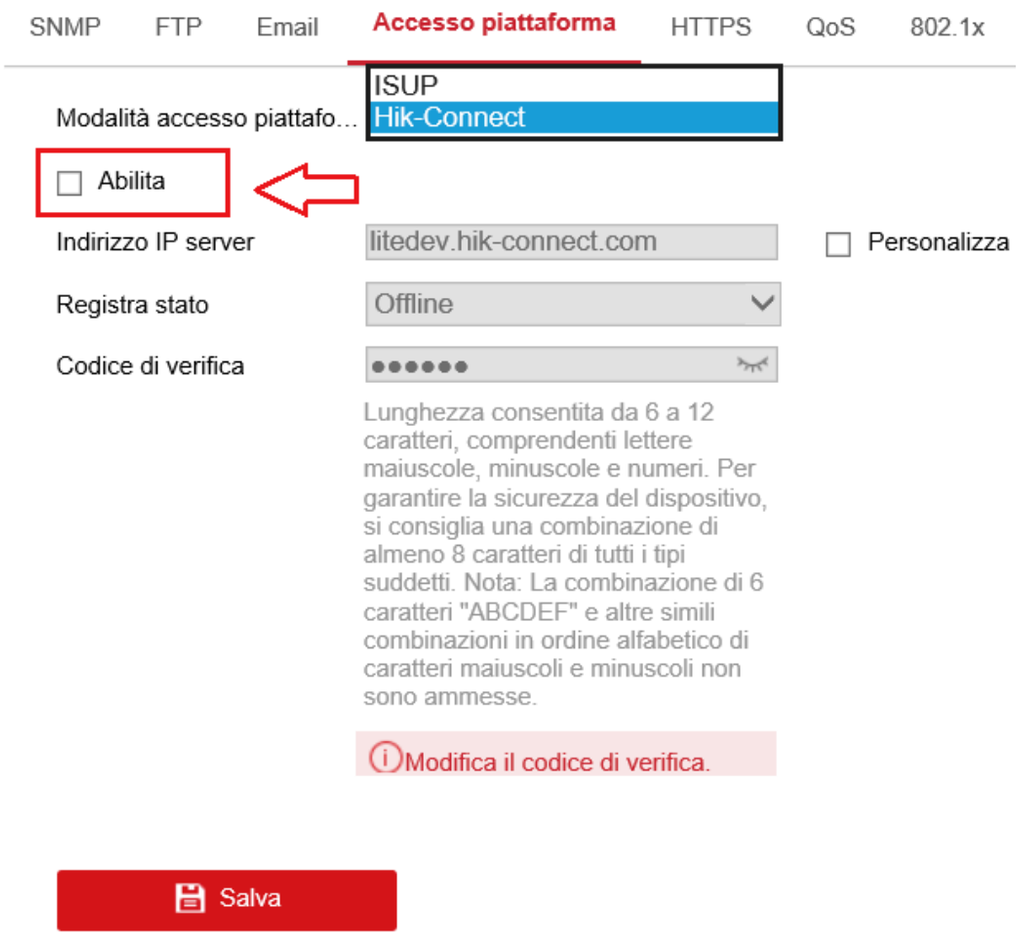
UPnP Plug&Play (protocollo di negoziazione dati per la pubblicazione e visualizzazione da remoto)

A seconda di come è stato predisposto il sistema di videosorveglianza, inclusa la negoziazione dei dati con il dispositivo che filtra le comunicazioni con l'esterno, questa funzione può rimanere disabilitata o meno.

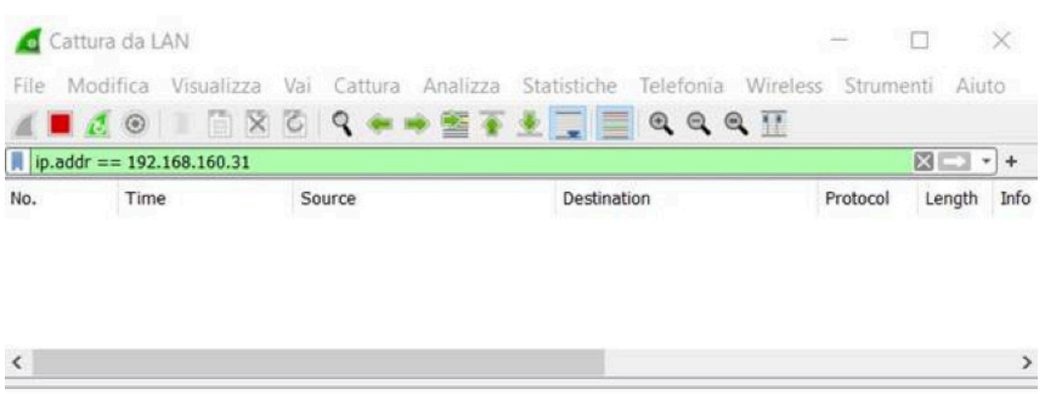


Tipo Porta	Porta Esterna	Indirizzo IP esterno	Porta interna	Stato
HTTP	80	0.0.0.0	80	Non valido
HTTPS	443	0.0.0.0	443	Non valido
RTSP	554	0.0.0.0	554	Non valido
Porta Server	8000	0.0.0.0	8000	Non valido

CLOUD/EHOME (protocollo per la remotizzazione del dispositivo)



Attraverso l'utilizzo di un software di sniffing della rete, otteniamo evidenza di una completa assenza di comunicazione con l'esterno:



Ne consegue che, disabilitando i suddetti protocolli e funzionalità, non si ottengono le informazioni menzionate durante la trasmissione televisiva. Per quel che riguarda il servizio Cloud, questo transita per server Europei localizzati in Irlanda in conformità al GDPR e all'interno degli stessi non vi è alcuna archiviazione di immagini e/o video. La riconducibilità della proprietà del Cloud agli HQ di Hikvision in Cina è corretta e sarebbe scorretto, oltre che futile, celarla.

E ribadiamo con fermezza l'inattendibilità di quanto diffuso dalle testate giornalistiche riguardo alla rimozione/sostituzione delle telecamere Hikvision dai locali del Parlamento Europeo e riguardo all'avvio, da parte dei funzionari di Camera e Senato, di procedure finalizzate alla rimozione/sostituzione delle stesse.

NOTE

NOTE

www.hikvision.it