IL RITORNO DEL DRAGONE
di Giulio Valesini e Cataldo Ciccolella
Collaborazione di Eleonora Zocca e Norma Ferrara
Immagini Paolo Palermo – Fabio Martinelli
Montaggio Riccardo Zoffoli

GIULIO VALESINI FUORI CAMPO
La Rai è un'azienda strategica del nostro paese. Il fornitore principale delle telecamere intelligenti è la Hikvision. Lo stato cinese ne ha il controllo societario con una quota del 42%. Abbiamo deciso di fare un esperimento: con un consulente esperto in cyber security siamo penetrati dentro il sistema di videosorveglianza della Rai per capire cosa accade ai dati catturati dalle telecamere ogni volta che riescono a connettersi alla rete.

FRANCESCO ZORZI – ESPERTO CYBERSICUREZZA
Questi sono gli indirizzi IP locali che stanno comunicando sia in broadcast ma anche con l'esterno. Quelle che prima stavano provando a cercare di comunicare, adesso iniziano a comunicare.

GIULIO VALESINI
Dove sono piazzati?

FRANCESCO ZORZI – ESPERTO CYBERSICUREZZA
Questi sono quelli dove ci sono accessi praticamente delle persone, dunque sistemi di controllo dei badge piuttosto che tornelli.

GIULIO VALESINI
Sono quelle telecamere che inquadrano i volti di chi entra e di chi esce?

FRANCESCO ZORZI – ESPERTO CYBERSICUREZZA
Esatto. E trovano delle comunicazioni verso dei server che sono registrate in sostanza dalla Hikvision e sono di Zhejiang.

GIULIO VALESINI FUORI CAMPO
La scoperta è inquietante. Il sistema in teoria è chiuso, ma se lo si apre a internet, come ad esempio per una manutenzione, in pochi minuti vede migliaia di tentativi di comunicazione con l'esterno, delle telecamere che puntano gli ingressi del centro di produzione della Rai. I dati sensibili delle persone che entrano, quindi, sono accessibili dall'esterno e vengono inviati proprio in Cina.

FRANCESCO ZORZI –ESPERTO CYBERSICUREZZA
Esatto, comunicano con i server che abbiamo rilevato essere registrato da Alibaba cloud computing in Cina.

GIULIO VALESINI
Quindi queste telecamere dialogano con server in Cina.

FRANCESCO ZORZI – ESPERTO CYBERSICUREZZA

Dialogano con server che alla fine il server primario è un server statunitense, seguono poi, sono riconducibili…

GIULIO VALESINI
Il messaggio finale arriva in Cina?

FRANCESCO ZORZI – ESPERTO CYBERSICUREZZA
Sì, sono registrate proprio da un ente collocato in Cina.

SIGFRIDO RANUCCI IN STUDIO
Dunque i nostri dati sensibili vengono inviati verso un server che è registrato negli Stati Uniti e poi finiscono in Cina, in una regione dove ha sede proprio la Hikvision, la casa madre delle telecamere. Avevamo all'epoca allertato subito la security Rai che aveva posto immediatamente rimedio. Però da quel momento in poi abbiamo ricevuto delle segnalazioni che ci hanno fatto capire che quello non era un caso isolato. E il tenore delle mail che sono arrivate in redazione era proprio questo: "avete colto nel segno, per quello che riguarda le telecamere di videosorveglianza, ogni tanto tentano di connettersi con dei server esterni al nostro paese e tentano di inviare informazioni". Ora tra le segnalazioni ce ne è una che è forse la più inquietante: quella che riguarda l'aeroporto di Fiumicino, quando 140 telecamere tutte insieme all'improvviso hanno tentato di connettersi più volte ma non poche volte, in maniera intensa complessivamente oltre un milione e mezzo di volte – e hanno tentato di connettersi a un indirizzo IP fino a oggi sconosciuto. Hanno tentato di mandare dati sensibili oppure c'è stato qualcuno che da remoto ha tentato di controllare la rete di videosorveglianza di un luogo strategico per il Paese? Fatto sta che questo è un fatto che apre degli scenari abbastanza inquietanti e che è diventato oggetto di attenzione dei nostri apparati di sicurezza. I nostri Giulio Valesini e Cataldo Ciccolella.

GIULIO VALESINI FUORI CAMPO
Aeroporto internazionale di Fiumicino. Il più grande d'Italia. Nel 2019, prima del Covid, da qui sono transitate quasi 45 milioni di persone che vengono videoriprese anche per prevenire attacchi terroristici. Ci sono telecamere ovunque, soprattutto di Hikvision.

Pubblicità

SIGFRIDO RANUCCI IN STUDIO
Bentornati, allora parliamo di telecamere di siurezza. Un anno fa avevamo scoperto che le telecamere Hikvision montate in Rai, ogni tanto cercavano di dialogare all'esterno mandando informazioni su server che erano registrati negli Stati Uniti e poi andavano in Cina, proprio in quelle regioni dove c'era casa madre Hikvision. Poi avevamo avvisato la nostra security che aveva posto immediatamente rimedio ma successivamente abbiamo scoperto che non era un caso isolato. E' successo anche a Fiumicino dove 140 telecamere Hikvision ad un certo punto hanno cominciato a tentare di collegarsi ad un sito che aveva un IP sconosciuto e lo hanno fatto anche con una certa insistenza, oltre 1 milione mezza di volte non sappiamo se per mandare informazioni o se era in corso un attacco informatico per controllare, gestire le telecamere di videosorveglianza di un luogo strategico per il nostro paese. In seguito proprio a questa nostra denuncia, Consip che è la centrale per gli acquisti della pubblica amministrazione prima dell'imminenza della chiusura di una gara da 65 milioni di euro che avrebbe comportato l'installazione di telecamere nelle nostre pubbliche amministrazioni, nei comuni, negli enti, negli immobili della pubblica amministrazione, visto che c'era una vulnerabilità ha chiesto come comportarsi al DIS, cioè ai nostri servizi di sicurezza. Questo perché le telecamere

fabbricate in Cina hanno una vulnerabilità per legge se costrette, devono dare i dati a Pechino. Ora in questo periodo poi è successo anche che alcune telecamere fabbricate in Cina come Hikvision hanno sostanzialmente perso il certificato ONVIF che è un certificato che certifica la loro abilità a "dialogare" con telecamere di altri marchi. Ora questo comporta una grana in casa CONSIP tutta da gestire e poi come la mettiamo con le telecamere che sono state già installate?

GIULIO VALESINI FUORI CAMPO
È il primo aprile del 2015, al sistema di videosorveglianza succede qualcosa di anomalo. Un responsabile della rete informatica si accorge di una grave anomalia nel funzionamento di oltre cento telecamere. Manda un alert interno di cui Report è entrato in possesso. È un'e-mail indirizzata alla Sigma spa. La società che aveva l'appalto per l'installazione delle telecamere che controllavano tutte le scale mobili di Fiumicino. Il documento avvisava: "C'è un problema urgente con le telecamere Hikvision"

MASSIMILIANO CESARONI – AMMINISTRATORE DELEGATO SIGMA SPA
Mandavano richieste di connessione ad un particolare indirizzo IP la cui sigla mi sembra cominciasse per 192.

GIULIO VALESINI
Corretto.

MASSIMILIANO CESARONI AMMINISTRATORE DELEGATO SIGMA SPA
La ripetizione di ricerca di questo indirizzo che fa pensare che questo indirizzo non fosse configurato nel sistema di videosorveglianza.

GIULIO VALESINI
Cercavano di registrarsi presso un server esterno.

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
Bisognerebbe capire chi aveva in carico sto indirizzo.

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
Di chi è 'sto indirizzo?

GIULIO VALESINI
Ma se Fiumicino chiede a voi, evidentemente a Fiumicino non gli tornava.

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
è come se l'ufficio di urbanistica di Roma mi chiede qual è l'indirizzo tuo, suo.

GIULIO VALESINI
Lei dice che ma ne so io.

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
Lo dovreste sapere voi, insomma.

GIULIO VALESINI
Esatto.

GIULIO VALESINI FUORI CAMPO

La richiesta di intervento partita da ADR TEL, la società che gestisce i sistemi informatici di Fiumicino, era urgente. Ognuna delle 140 telecamere Hikvision presenti nello scalo romano inviava quattro richieste di apertura di una connessione verso l'esterno. 11mila a telecamera ogni ora. Più di un milione e mezzo in totale. Un traffico enorme da bloccare che stava mettendo in difficoltà il sistema di sicurezza dell'aeroporto. La segnalazione in quelle ore fu girata anche alla GSG, la società italiana che gestiva i software del sistema di videosorveglianza.

GIULIO VALESINI
A me è arrivata questa email. Aprile 2015. Circa 11 mila richieste l'ora di comunicazione con l'esterno di 140 telecamere.

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
(silenzio) mmh.

GIULIO VALESINI
Lei che all'epoca lavorava lì all'aeroporto questa storia se la ricorda o no, la conosce o no?

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Effettivamente abbiamo visto che il problema era esistente ma che non dipendeva dal software, dipendeva da queste telecamere che cercavano di dialogare con un server esterno all'aeroporto. Per fare questa cosa cercavano di aprire una porta per uscire e giustamente il firewall dell'aeroporto diceva.

GIULIO VALESINI
Dove vai?

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Dove stai andando? Lì è una rete chiusa.

GIULIO VALESINI
Che tipo di messaggio era?

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Certamente non era un bug.

GIULIO VALESINI
Secondo lei che cosa c'è dietro?

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Per la nostra conoscenza, quindi direi una cosa direi certa, la trasmissione che avvenne non mandavano immagini

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
La cosa potenzialmente possibile è che se io conosco l'indirizzo, ho tutta una serie di computer che rispondono a me, io gli posso aggiornare il software oppure gli posso dire: tu telecamera attacca i server dell'aeroporto.

GIULIO VALESINI
E a quel punto che succede?

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Se 400, 500, 1000 telecamere all'interno di una rete, magari anche chiusa, protetta, iniziano a fare traffico anomalo.

GIULIO VALESINI
Il sistema crasha.

ANTONMARIO CATANIA – PRESIDENTE GSG INTERNATIONAL
Potenzialmente una telecamera che risponde ai miei comandi è come se fosse come dire una cellula dormiente.

GIULIO VALESINI FUORI CAMPO
Il sospetto è che la rete di telecamere possa essere usata come una botnet per attacchi informatici verso l'esterno. Significa che le camere vengono prima infettate e poi trasformate in un robot a comando di un malintenzionato che da remoto, all'insaputa del produttore e dell'utilizzatore, le userà per colpire altre reti o sistemi informatici, magari proprio dell'aeroporto, che saranno messi ko, colpiti da decine di migliaia di tentativi di comunicazione. A Roma incontriamo un importante operatore del settore della videosorveglianza. Conosce l'incidente di Fiumicino e, a quanto ci dice, la questione arrivò anche all'orecchio dei nostri servizi di intelligence. La spiegazione di un semplice bug delle telecamere non aveva convinto.

DIRIGENTE SOCIETA' VIDEOSORVEGLIANZA
Dopo gli eventi di Fiumicino ho avuto un colloquio con un esponente dei servizi di intelligence, e abbiamo parlato di Hikvision. Mi risulta che in seguito i servizi hanno fatto circolare una nota interna dicendo "state attenti, non usate quella roba là".

GIULIO VALESINI FUORI CAMPO
Abbiamo mostrato la mail interna di fiumicino anche a Francesco Zorzi, il consulente di diverse procure italiane, specialista in cyber intelligence, che ha scoperto per noi di Report le anomalie nelle telecamere di Hikvision all'interno del sistema di videosorveglianza della Rai. Che ci fornisce un'altra lettura dei fatti.

FRANCESCO ZORZI - ESPERTO CYBERSICUREZZA
Se io riesco a fare un attacco, ad esempio, di flooding interno alla rete e, ad esempio, saturare il traffico di una specifica videocamera, io impedisco a questa videocamera riesca in sostanza a comunicare, impedisco di far sì che quel dispositivo in quel momento registri.

GIULIO VALESINI
Quindi se io avessi voluto in quel momento forse bucare il sistema, cioè quindi passare per Fiumicino.

FRANCESCO ZORZI - ESPERTO CYBERSICUREZZA
Con questo l'avrei fatto sicuramente.

GIULIO VALESINI FUORI CAMPO
Un attacco per far passare qualcuno senza che venisse registrato dalle telecamere. È una delle possibilità. Ma quello che è certo è pur se il misterioso incidente rilevato alle telecamere di sorveglianza di Fiumicino non sia mai stato mai reso noto, la questione non passò inosservata nell'ambiente della cybersicurezza. L'eco superò l'oceano, arrivò in Canada, al quartiere generale della Genetec, un gigante mondiale delle tecnologie per la sicurezza.

PIERRE RACZ – PRESIDENTE GENETEC
Sono rimasto sorpreso da quell'incidente. Il dipartimento IT dell'aeroporto conta su persone capaci e ci hanno coinvolto per trovare una soluzione. Noi, dopo quell'incidente, abbiamo smesso di supportare Hikvision.

GIULIO VALESINI
Se lei fosse il ministro dell'Interno italiano che sa che queste telecamere sono presenti nei tribunali, nelle questure, nelle forze di polizia, oggi sarebbe tranquillo?

PIERRE RACZ – PRESIDENTE GENETEC
No, no. Non sarei affatto a mio agio. Quello che farei sarebbe adottare una strategia di gestione del rischio. Identificare dove si è più vulnerabili, e poi procedere con un piano di contenimento e progressiva sostituzione delle telecamere.

CATALDO CICCOLELLA
Abbiamo visionato della documentazione che dimostra come il primo aprile del 2015 l'aeroporto di Fiumicino abbia visto circa 140 telecamere Hikvision aprire nel giro di un'ora più o meno un milione e mezzo di tentativi di comunicazione verso un IP sconosciuto.

ENRICO BORGHI – COMITATO PARLAMENTARE PER LA SICUREZZA - PARTITO DEMOCRATICO
Le devo dire che non mi meraviglio. Grazie anche al vostro lavoro era emerso che una situazione analoga aveva addirittura coinvolto l'azienda di Stato sulle telecomunicazioni cioè la Rai. In Cina questo tipo di attività non solo è consentito. In Cina questo tipo di attività è pianificato, organizzato e messo in campo nell'ambito di una specifica organizzazione della società cinese.

GIULIO VALESINI FUORI CAMPO
Pochi giorni fa Borghi ha presentato un'interrogazione parlamentare sulla sicurezza delle telecamere Hikvision. Ha usato Shodan, una specie di mappa di tutti gli oggetti connessi al web, facendo una scoperta preoccupante: migliaia di dispositivi Hikvision sono esposti in rete. Così, anche le telecamere che sorvegliano le nostre case sono rintracciabili e quelle con vulnerabilità perfino attaccabili. Un intruso potrebbe facilmente vedere a che ora usciamo di casa o con chi stiamo parlando in giardino.

ENRICO BORGHI – COMITATO PARLAMENTARE PER LA SICUREZZA - PARTITO DEMOCRATICO
Noi abbiamo verificato che queste telecamere avevano un meccanismo di riversamento dati che non corrisponde agli standard e alle esigenze che si debbono garantire nel nostro Paese.

GIULIO VALESINI FUORI CAMPO
È quello che è successo anche all'aeroporto di Fiumicino.

GIULIO VALESINI
Il bando di gara imponeva Hikvision o voi avete scelto telecamere Hikvision in base ad una convenienza economica?

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
Il listino esplicitava già dei modelli Hikvision con delle caratteristiche, ma reputo quasi impossibile trovare qualcosa con caratteristiche migliorative di Hikvision a un prezzo inferiore.

GIULIO VALESINI
Quindi diciamo che fu una scelta obbligata, lo possiamo dire?

MASSIMILIANO CESARONI - AMMINISTRATORE DELEGATO SIGMA SPA
Su alcuni modelli forse è quasi obbligata.

SIGFRIDO RANUCCI IN STUDIO
Allora ci ha scritto ADR aeroporti di Roma e dice che "rispetta da sempre tutte le norme e regolamenti in materia di security e assicura le massime tutele previste dalla regolazione di settore in materia di gestione e tutela dei dati, utilizzando delle telecamere, scrivono, di sicurezza che rispettano i requisiti dettati dalla normativa e dagli Enti di riferimento". Ora questo ci fa piacere, ma non spiegano che cosa effettivamente è successo quel giorno quando le 140 telecamere hanno cominciato a tentare di connettersi e mandare forse informazioni all'esterno. Ecco e quello che noi invece abbiamo scoperto, i nostri Giulio Valesini e Cataldo Ciccolella, è che non si tratta di un caso isolato neppure questo. Perché pochi giorni fa l'azienda di cybersecurity Fortinet ha scoperto che migliaia e migliaia di telecamere Hikvision stanno subendo un attacco informatico da una botnet, cioè da una rete robotica che viene utilizzata dagli hacker probabilmente per sottrarre delle informazioni sensibili oppure per attaccare dei siti strategici. Ora siccome questa cosa sta andando avanti già da un bel po' di tempo, ed è tutt'ora in corso la domanda lecita è: questo attacco avviene perché c'è un bug che è stato scoperto nel settembre del 2021 su queste tipologie di telecamere. Quante ce ne sono nel nostro paese, quante ne ha la nostra pubblica amministrazione. Cioè quante di queste telecamere sono infette già o potrebbero essere infettate?

GIULIO VALESINI FUORI CAMPO
Con la pandemia anche i rilevatori di temperatura si sono moltiplicati, e con loro l'intelligenza artificiale che studia e analizza ogni immagine. Ma dietro quegli occhi, ci sono le leggi sulla sicurezza emanate da Pechino nel 2017. Impongono di rivelare informazioni sensibili qualora vengano richieste dal governo.
In Italia Hikvision è leader del mercato. Negli anni ha piazzato le sue telecamere nei luoghi strategici per la sicurezza nazionale. Non solo aeroporti come Malpensa e Fiumicino ma anche i palazzi delle istituzioni politiche, tribunali, forze dell'ordine. Hikvision Italia è posseduta da una holding europea, a sua volta detenuta dalla casa madre cinese. Anche gli amministratori della Srl italiana sono cittadini cinesi. Il controllo di Hikvision è nelle mani del CETC, un'azienda dello stato cinese che sviluppa software militari, infrastrutture di difesa, armi elettroniche. Insomma, Hikvision è nelle mani di un gigante strettamente legato all'esercito cinese. L'amministratore è Chen Zong Nian, è un parlamentare del partito comunista cinese.

GIULIO VALESINI
è vero che la Cina sono già 7,8 anni che invece a sua volta ha vietato per il controllo di aree sensibili, strategiche dal punto di vista militare, l'uso di telecamere che non siano cinesi?

GIULIO VALESINI FUORI CAMPO
In Inghilterra, questa estate, un attivista per i diritti umani ha chiesto l'accesso agli atti all'ufficio del primo ministro inglese: voleva sapere se e dove il governo usava telecamere Hikvision. La risposta, rivelata poche settimane fa, è che non ne utilizzano e che anzi, l'indirizzo del ministero della Difesa, che decide l'installazione, è di non usare Hikvision".

CHARLES ROLLET - IPVM
Il Regno Unito, ma anche gli Stati Uniti, l'Australia e Taiwan hanno bandito Hikvision dalle loro infrastrutture militari.

CHARLES ROLLET - IPVM
Sì, la Cina, nel 2012, ha deciso che le telecamere di sorveglianza straniere erano un rischio per la sicurezza cinese, e così hanno blindato tutti i network governativi.

GIULIO VALESINI FUORI CAMPO
A giugno 2021, dopo che Report aveva mostrato le anomalie dei dispositivi di videosorveglianza Hikvision piazzati in Rai, Consip ha preso in mano lo scottante dossier. La prima gatta da pelare è la gara da 65 milioni di euro per la videosorveglianza, aggiudicata in modo quasi definitivo a ottobre. I vincitori si apprestavano a installare massicciamente prodotti Hikvision. Allora Consip si è rivolta ai servizi di intelligence e all'agenzia per la cybersicurezza.

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Noi abbiamo avuto un'interlocuzione con questi soggetti preposti per la sicurezza nazionale. Ai soggetti aggiudicatari di questi dieci lotti gli chiederemo se rispetto a questi punti che ci sono stati sottoposti come condizione…

GIULIO VALESINI
Ma quali sono queste condizioni?

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Le funzioni di comunicazione con l'esterno, il fatto di poter disabilitare l'amministratore di sistema, di disabilitare queste funzioni.

GIULIO VALESINI
Sulle telecamere di Hikvision, Dahua, di una certa provenienza, avete alzato il livello di sorveglianza, di allerta?

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Assolutamente, i punti sono quelli che voi sapete bene che avete già evidenziato nei vostri servizi.

GIULIO VALESINI
E se non li rispettano?

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Se non dovessero rispettarli, noi renderemo noto in sede di aggiudicazione quindi daremo pubblicità alle amministrazioni che così sanno cosa comprano. Quando lei su un pacchetto di sigarette legge nuoce gravemente alla salute, lei che fa?

GIULIO VALESINI FUORI CAMPO
Gli obiettivi da proteggere del nostro paese sono dentro un perimetro che è segreto, ma anche molto ristretto. Lascia fuori migliaia di siti comunque sensibili come tribunali, caserme, aeroporti e le stazioni ferrovieri e molto altro ancora. Da questa estate tutto, però, passa per l'Agenzia per la cybersicurezza nazionale, voluta da Mario Draghi. Alla guida c'è Roberto Baldoni, uno dei massimi esperti italiani, viene dal DIS – il Dipartimento delle informazioni per la sicurezza - il coordinamento dei nostri servizi segreti. Deve mettere in sicurezza un Paese che per anni ha trascurato i rischi informatici.

GIULIO VALESINI
Se io poi mi guardo intorno vedo che in tutti i luoghi sensibili di sicurezza nazionale del nostro Paese ci sono le stesse telecamere che poi hanno dato nel tempo questo tipo di problemi qua e che negli altri paesi sono, come dire, guardate con una certa diffidenza…

ROBERTO BALDONI – DIRETTORE AGENZIA CYBERSICUREZZA NAZIONALE
In particolare, per quanto riguarda gli Stati Uniti, la sicurezza nazionale permette per esempio di realizzare delle liste un po' di proscritti all'interno diciamo dei settori in particolare dell'alta tecnologia. In Europa non esiste. Quello che si sta mettendo ora su in Europa è un contesto di certificazione di cybersecurity.

GIULIO VALESINI
Queste telecamere hanno mostrato delle continue vulnerabilità, come pensate di proteggere gli obiettivi sensibili del nostro Paese?

ROBERTO BALDONI – DIRETTORE AGENZIA CYBERSICUREZZA NAZIONALE
C'è una gestione del rischio che viene fatta rispetto a due cose fondamentali: l'oggetto che, diciamo, devo installare e due, dove lo vado a installare.

GIULIO VALESINI
Al momento non c'è differenza tra un tribunale e un piccolo ente locale. cioè, la logica è quella commerciale?

ROBERTO BALDONI – DIRETTORE AGENZIA PER LA CYBERSICUREZZA NAZIONALE
E' una problematica che dovremo affrontare probabilmente nel futuro.

GIULIO VALESINI
Lei conosce il fatto che queste società anche se operano in Italia sono soggette all'obbligo in caso di richiesta del governo cinese di passare informazioni acquisite nell'ambito delle loro funzioni anche con l'Italia.

ROBERTO BALDONI – DIRETTORE AGENZIA CYBERSICUREZZA NAZIONALE
Se lei va a leggere il Dpcm che definisce le misure di sicurezza del perimetro noterà che ci sono, diciamo, delle misure di sicurezza molto chiare per quanto riguarda sia la gestione dei dati sia per quanto riguarda la supply chain dal punto di vista dei dispositivi. Dateci tempo.

GIULIO VALESINI FUORI CAMPO
Dal luglio 2020 le telecamere cinesi non hanno più la certificazione ONVIF: è il nome del consorzio che dà il bollino e che è, sulla base delle restrizioni decise dal governo americano, non assicura più che le telecamere Hikvision e di altri marchi, parlino la stessa lingua dei prodotti usati nella pubblica amministrazione italiana. Tra questi c'è la Dahua Technology. In Italia gli affari stanno andando a gonfie vele: un terzo delle telecamere vendute ha il loro brand. Sorvegliano la città del Vaticano. A settembre dello scorso anno hanno piazzato 19 termoscanner a riconoscimento facciale a Palazzo Chigi. Eravamo andati a trovarli.

GIULIO VALESINI
Lei conosce le leggi sulla sicurezza in Cina?

PASQUALE TOTARO – GENERAL MANAGER DAHUA TECHNOLOGY ITALIA
No. Conosco a malapena quelle italiane perché nessuno è venuto a dirmi "Pasquale tu devi far sì che devi dare informazioni o devi…"

GIULIO VALESINI
Magari non gliel'hanno detto, ha capito.

PASQUALE TOTARO – GENERAL MANAGER DAHUA TECHNOLOGY ITALIA
Eh, allora come faccio a rispettare una regola che non me l'hanno detta…

GIULIO VALESINI FUORI CAMPO
Il presidente della Dahua italiana è Fu Liquan: è un cittadino cinese, principale azionista del gruppo. Difficile che possa disobbedire al governo mettendo a rischio libertà e miliardi. Oggi a distanza di un anno hanno perso la certificazione Onvif.

PASQUALE TOTARO – GENERAL MANAGER DAHUA TECHNOLOGY ITALIA
Abbiamo richiesto la certificazione alla Onvif che ci ha comunicato e confermato che fino a dicembre 2022 noi siamo membri dell'Onvif come full.

GIULIO VALESINI
Perché a noi invece ci ha comunicato che voi, Hikvision, non avete più la possibilità di certificare i vostri prodotti ormai da circa luglio 2020, quindi.

PASQUALE TOTARO – GENERAL MANAGER DAHUA TECHNOLOGY ITALIA
A noi ad oggi risulta l'esatto opposto, poi se così non dovesse essere… a questo punto comincio a vedere una certa discriminazione razziale di una forzatura del genere.

GIULIO VALESINI
Quindi lei dice è una discriminazione in quanto siete un'azienda cinese.

PASQUALE TOTARO – GENERAL MANAGER DAHUA TECHNOLOGY ITALIA
Sì, perché non c'è nessun termine tecnico che vada ad avvalorare l'esclusione dall'Onvif dal punto di vista di sicurezza. Se me la trovano io sarò il primo a dire "fate benissimo perché per me la sicurezza è importante, non solo per me ma per tutti quanti. Ma se non me la trovano allora ho ragione io.

GIULIO VALESINI FUORI CAMPO
C'è un piccolo dettaglio: nella mega gara Consip per il rinnovo delle telecamere di videosorveglianza nella pubblica amministrazione, ormai conclusa, la certificazione ONVIF è un requisito necessario e non averla è un problema.

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Si chiama evoluzione tecnologica. Quando c'è l'evoluzione tecnologica, il fornitore ci dice "non ho più la certificazione" quindi non rispetta più i requisiti tecnici di gara.

GIULIO VALESINI
Il contraente.

CRISTIANO CANNARSA – AMMINISTRATORE DELEGATO CONSIP
Il contraente ti dice ti do un prodotto dello stesso vendor però certificato. Oppure se non riesce perché non ha più la certificazione ti da il prodotto di un altro vendor, quindi un'altra telecamera in questo caso, che avrà la certificazione.

GIULIO VALESINI
Mr. Pierre Racz noi sappiamo che alcune società di proprietà cinese da luglio 2021 non hanno più certificati ONVIF. Secondo voi che tipo di problema ci può essere per chi utilizza questi prodotti?

PIERRE RACZ – PRESIDENTE GENETEC
Avranno grandi difficoltà ad integrarli con altri dispositivi. E tutti i clienti che hanno ancora quelle telecamere non saranno in grado di aggiornare il firmware senza perdere la certificazione. Si crea una vulnerabilità enorme. Pochi giorni fa il direttore del MI6, i servizi segreti inglesi, ha dato un avvertimento: la strategia dell'intelligence di certi paesi è quella di rifilare trappole cattura-dati. L'Italia è una potenza mondiale del pensiero creativo, del design... se non difendete i dati su cui si basa tutto questo, sarà a rischio la vostra prosperità.

SIGFRIDO RANUCCI IN STUDIO
E' un problema che coinvolge tutta l'Europa tranne per i siti super sensibili, quelli strategici che sono tutelati da un perimetro della sicurezza cibernetica in base alle nuove disposizioni. Il cerino bollente però rimane in mano alla pubblica amministrazione perché in base ai regolamenti europei alle gare possono partecipare tutte le ditte cinesi compresi. Cosa diversa nella Gran Bretagna dove il ministero della Difesa ha un dipartimento ad hoc che si occupa di installare le telecamere e nei luoghi sensibili e hanno deciso di non installare telecamere Hikvision. Sono corsi ai ripari anche gli Stati Uniti e dal 2020 vietano praticamente di installare telecamere per quello che riguarda tutti i luoghi federali senza un'autorizzazione del ministero della Difesa nazionale. E hanno vietato l'installazione nei luoghi sensibili delle telecamere Dahua, Huawei e appunto Hikvision. Ora questo è un guaio che si prospetta in previsione del futuro digitale. Dove passa anche un pezzo della nostra salute.