KIBERDROŠĪBA

Videonovērošanas ierīču nodrošināšana, lai novērstu tīkla ievainojamību.

2020. gada 17. novembris

Autortiesības ⓒ 2024 Hanwha Vision Co., Ltd. Visas tiesības aizsargātas.

SATURS

1.Ievads

Mēs dzīvojam arvien vairāk savienotā pasaulē, kurā arvien vairāk ierīču un sistēmu ir savienotas tīklā un koplietojamas ar citām sistēmām. Galvenais šīs tendences virzītājspēks ir ērtība, jo cilvēki ir sagaidījuši iespēju pieslēgties un kontrolēt ierīces un sistēmas jebkurā vietā un jebkurā laikā.

Tomēr arvien pieaugošais tīkla ierīču skaits nodrošina līdz šim nebijušas ērtības, proti, palielinās drošības risks. Tā kā katra ierīce ir tīkla galapunkts, tā potenciāli var kļūt par piekļuves punktu hakeriem un citām personām ar ļaunprātīgiem nodomiem. Patiesībā daudzos no pēdējā laikā notikušajiem skaļākajiem datu aizsardzības pārkāpumiem hakeri varēja piekļūt uzņēmumu tīkliem, izmantojot POS, *HVAC un citas tīkla sistēmas, kas nenodrošināja pietiekamu drošības līmeni, lai novērstu šāda veida pārkāpumus.

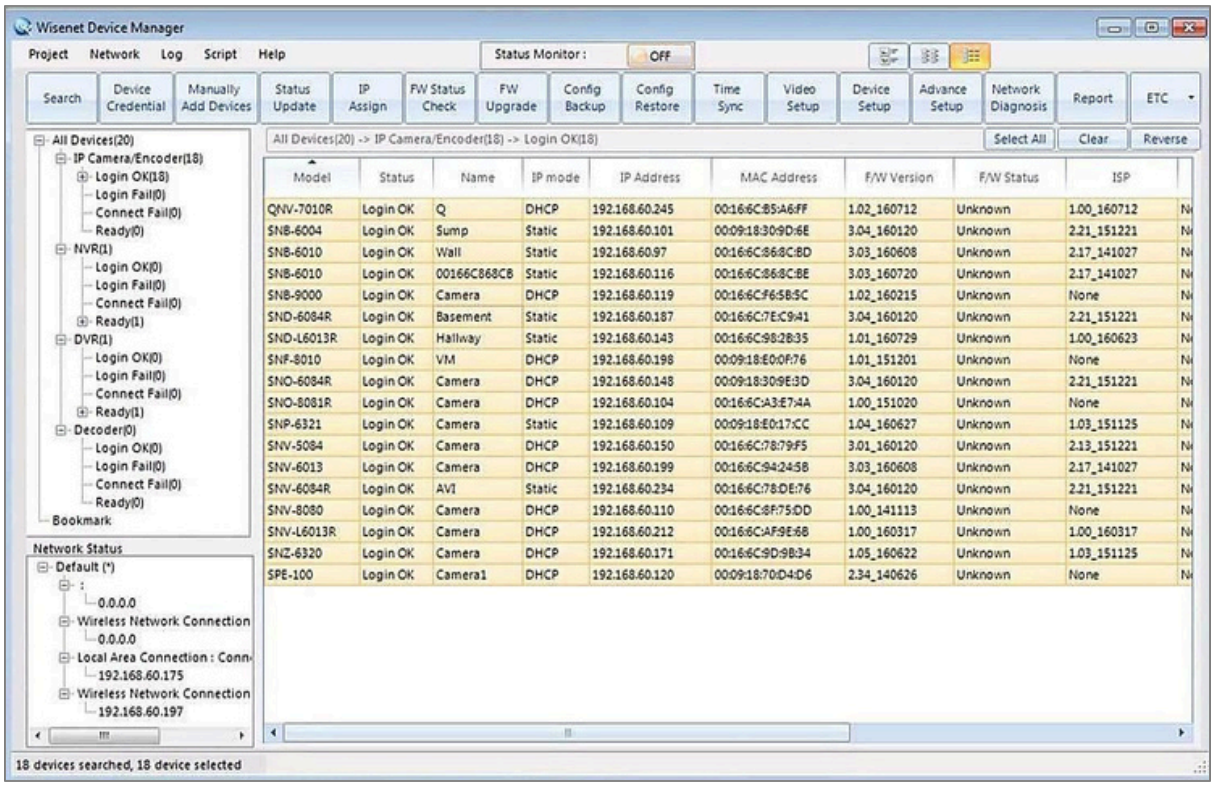
*HVAC: apkures, ventilācijas un gaisa kondicionēšanas sistēmas.

Lai gan IP videonovērošana un citi risinājumi ir kļuvuši arvien populārāki un kļuvuši par vispārpieņemtu standartu jaunai izvietošanai un modernizācijai, drošības sistēmas nav izņēmums. Hakeri neizšķir tīkla ierīces neatkarīgi no tā, vai tās pilda kritiski svarīgu funkciju, piemēram, drošības funkciju, vai nē. Tādējādi videonovērošanas kameras un citas ierīces ir garā potenciālo tīkla piekļuves punktu sarakstā, kas nepārtraukti tiek pārbaudīti, meklējot ievainojamības, kuras var izmantot. Tāpēc ir svarīgi, lai organizācijas veiktu nepieciešamos pasākumus, lai nodrošinātu visaugstāko drošības līmeni saviem tīkliem un IP kamerām, kodētājiem, NVR un DVR. Pastāv vairākas labākās prakses, kas būtu jāievēro, lai stiprinātu ierīču drošību, lai novērstu nesankcionētu piekļuvi un aizsargātu galalietotāju videonovērošanas sistēmas un to kopējo tīklu.

Hanwha Vision ne tikai zina par šo labāko praksi, bet savos produktos ir iestrādājusi vairākas tehnoloģijas un iespējas, lai organizācijām atvieglotu šo svarīgo soļu veikšanu tīkla drošības uzlabošanas virzienā.

Drošības sistēmu īpašniekam, IT personālam un sistēmu integratoriem, kas instalē sistēmas, jāpārskata šie elementi, lai noteiktu vajadzīgo drošības līmeni, vienlaikus līdzsvarojot lietošanas ērtumu un pieņemamos riskus. Šajā rokasgrāmatā attiecīgos gadījumos tiks parādīti tīkla kameru momentuzņēmumi. Lielāko daļu iestatījumu var konfigurēt partijas veidā vairākām kamerām, izmantojot Wisenet ierīces pārvaldnieka programmatūru (1. attēls).

1. attēls. Wisenet ierīces pārvaldnieka ekrāns



2. Parole

Paroles ir neatņemama mūsu ikdienas dzīves sastāvdaļa, sākot ar e-pasta pārbaudi un beidzot ar viedtālruņu atbloķēšanu vai pieslēgšanos datoriem. Tāpēc šķiet pietiekami intuitīvi, ka cilvēki apzinās, cik svarīgi ir izveidot spēcīgas paroles, lai aizsargātu savas ierīces un tīklus, taču realitātē tas ne vienmēr tā ir. Šī paraugprakse palīdzēs nodrošināt visaugstākā līmeņa paroļu drošību.

Ja ierīcēm, piemēram, kamerai un ierakstīšanas ierīcei, ir sākotnējā parole, lietotājam nevajadzētu izmantot sākotnējo paroli un iestatīt savu paroli, jo sākotnējā parole ir plaši pieejama, izmantojot lietotāja rokasgrāmatu vai internetu. Hanwha Techwin nenodrošina sākotnējo paroli, un visas ierīces ir paredzētas paroles iestatīšanai to sākotnējās lietošanas laikā.

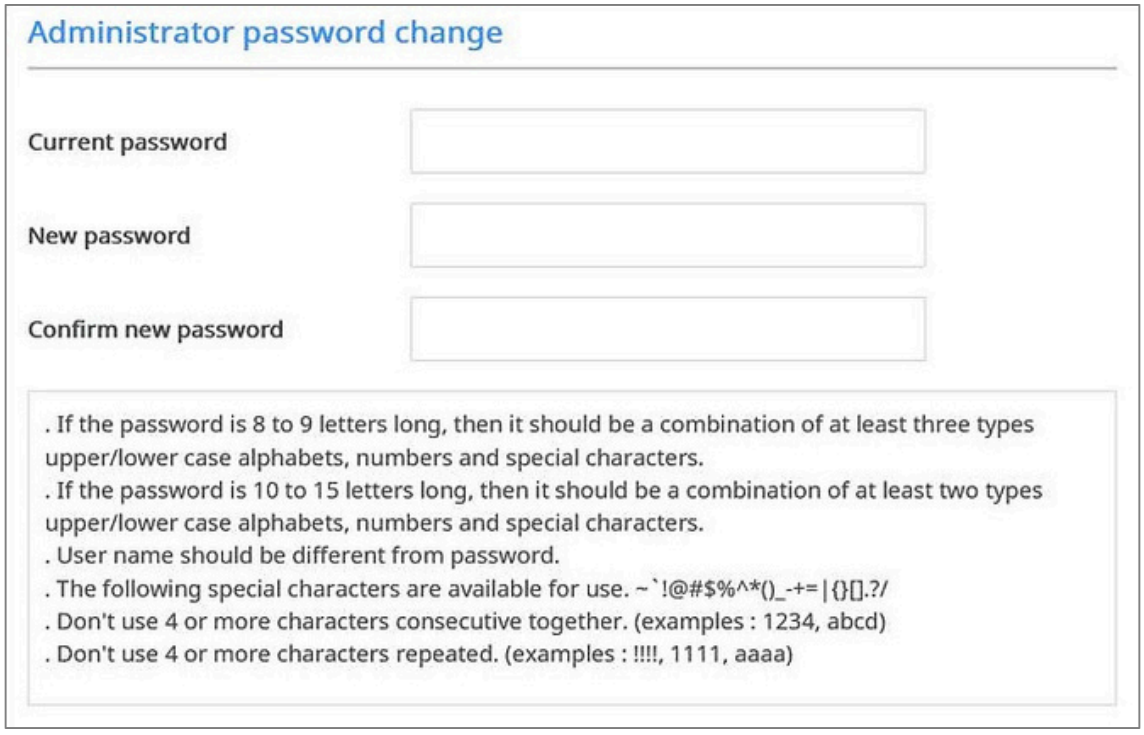
Tomēr ar paroles maiņu vien nepietiek. Jo daudzi cilvēki savas ērtības labad, iestatot paroli, ļoti bieži pieļauj divas kļūdas.

Pirmā ir vienas un tās pašas paroles lietošana visur. Bīstamība ir tāda, ka, ja kāds var atšifrēt, piemēram, jūsu e-pasta konta paroli, viņam ir piekļuve visam, ko esat aizsargājis ar paroli, un tas paver iespēju zādzībām, identitātes zādzībām un daudz kam citam. Otra - un visriskantākā - kļūda, ko cilvēki pieļauj, lai vieglāk atcerētos paroles, ir vārdu, dzimšanas datumu un/vai vārdu, kas atrodami vārdnīcā, izmantošana.

Hakeru uzlaušana ir kļuvusi par ļoti organizētu un izsmalcinātu praksi, kurā tiek izmantoti jaudīgi rīki, piemēram, tehnoloģijas, kas ātri un automātiski izraksta iespējamās vārdu kombinācijas, lai atšifrētu paroles. Šie rīki ir bijuši diezgan veiksmīgi ar viegli iegaumējamām parolēm, kas ir tik ērtas lietotājiem. Turklāt, tā kā tiešsaistē ir pieejams tik daudz personiskās informācijas, bez pūlēm var uzlauzt arī paroles, kurās izmantoti vārdi, dzimšanas dienas vai citi svarīgi datumi. Tādējādi ir obligāti jāizmanto spēcīgas paroles, kuras ir daudz grūtāk uzlauzt. Lai to panāktu, ir vairākas labākās prakses, kas jāievēro, izmantojot burtu, ciparu un citu simbolu kombināciju.

Lai gan tas nav obligāti, laba prakse ir arī izmantot atšķirīgas paroles katrai ierīcei vai izmantot vienu un to pašu paroli tikai dažām, nevis visām tīkla ierīcēm, klientiem un sistēmām. Ieteicams izveidot unikālu lietotājvārdu, nevis izmantot administratora kontu, ar kuru pieslēgties VMS un citiem klientiem. Tas novērš administratora paroles nepārtrauktu pārsūtīšanu tīklā, cenšoties novērst tās pārtveršanu.

Hanwha Vision produktiem nepieciešama 8 līdz 15 burtu gara parole. Ja parole ir 8 līdz 9 burtu gara, tai jābūt vismaz trīs veidu lielo/mazo burtu, ciparu un speciālo rakstzīmju kombinācijai. Ja paroles garums ir no 10 līdz 15 burtiem, tai jābūt vismaz divu veidu lielo/mazo burtu, ciparu un speciālo rakstzīmju kombinācijai. Turklāt parolei nevar izmantot secīgu vai atkārtotu teksta virkni.

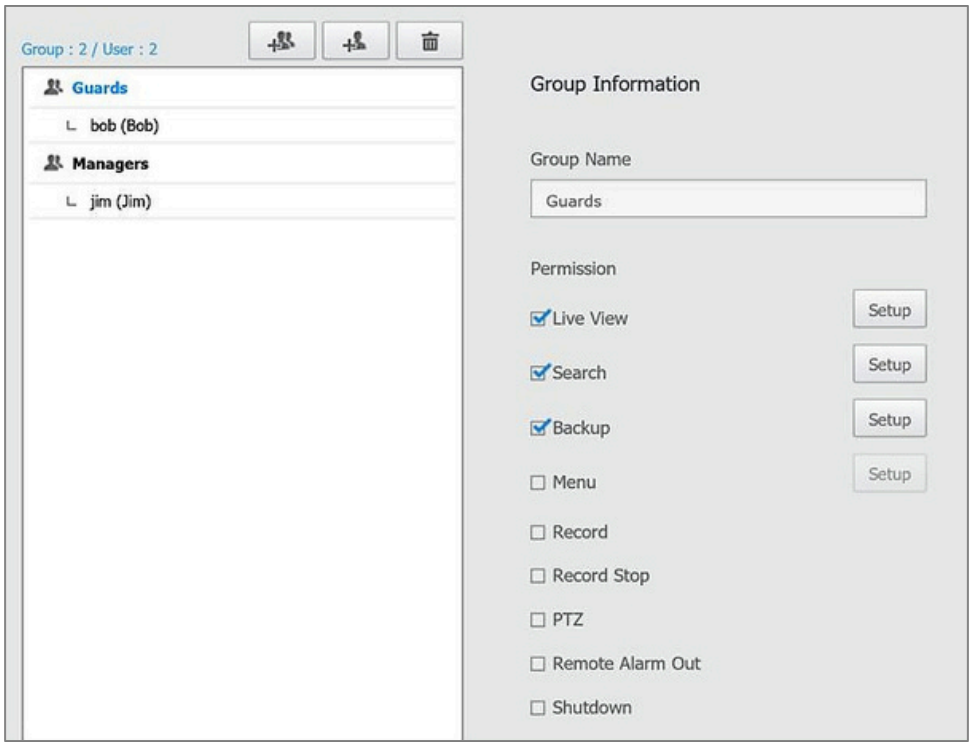


2. attēls. Kameras paroles konfigurēšana

Ierobežojot ar šo unikālo kontu saistīto autorizāciju, tiks ierobežota arī hakeru piekļuve. Tāpēc, ja konts tiks kompromitēts, tas neietekmēs visu kameru, tostarp tās iestatījumus. Turklāt unikālie pilnvarojumi padara žurnālu analīzi daudz vieglāku un informatīvāku. Hanwha Techwin kameras un ierakstītāji ļauj izveidot daudzas lietotāju/lietotāju grupas ar dažādām atļaujām un lietotāju līmeņiem.

3.1. MAZNOZĪMĪGĀKU PRIVILĒĢIJU PRINCIPS

Izmantojiet mazāko privilēģiju principu, nodrošinot lietotājam minimālās funkcijas, kas nepieciešamas, lai veiktu nepieciešamās funkcijas. Ja lietotājam reizi gadā ir nepieciešams piekļūt iestatīšanas izvēlnei, nodrošiniet alternatīvu lietotāja pieteikšanās iespēju, izmantojot tīmekļa saskarni, nevis ļaujiet lietotāja VMS kontam piekļūt pilnībā, vai, vēl labāk, uzdodiet augstāka līmeņa lietotājam veikt šo nerutīnisko uzdevumu. Tas palīdzēs novērst konfigurācijas izmaiņu veikšanu "no vietas" un pēc iespējas vairāk uzturēs augsta līmeņa akreditācijas datus ārpus tīkla.



3. attēls. SSM lietotāja autoritātes konfigurācija

3.2. Viesu piekļuve

Hanwha Vision kameras nodrošina atsevišķu viesa pieteikšanās funkciju ar lietotājvārdu un paroli "viesis". Šim kontam ir ierobežotas privilēģijas, un pēc noklusējuma tas ir neaktīvs, tāpēc tas ir īpaši jāieslēdz iestatīšanas izvēlnē. Tas ir ideāli piemērots ierobežotas piekļuves lietojumiem, taču, ja tas nav nepieciešams, tas ir jāizslēdz.

4.1. *Hešošana* pret atklātā teksta autentificēšanu

Lietotājvārdi un paroles tiek nosūtīti tīklos, izmantojot tīro tekstu, base64 kodējumu un HTTP protokolu pamata autentifikāciju, kas nodrošina atklātu piekļuvi šiem akreditācijas datiem jebkurai personai, kura uzrauga tīklu, lai pārtvertu un skatītu datplūsmu, ļaujot tai piekļūt ierīcei.

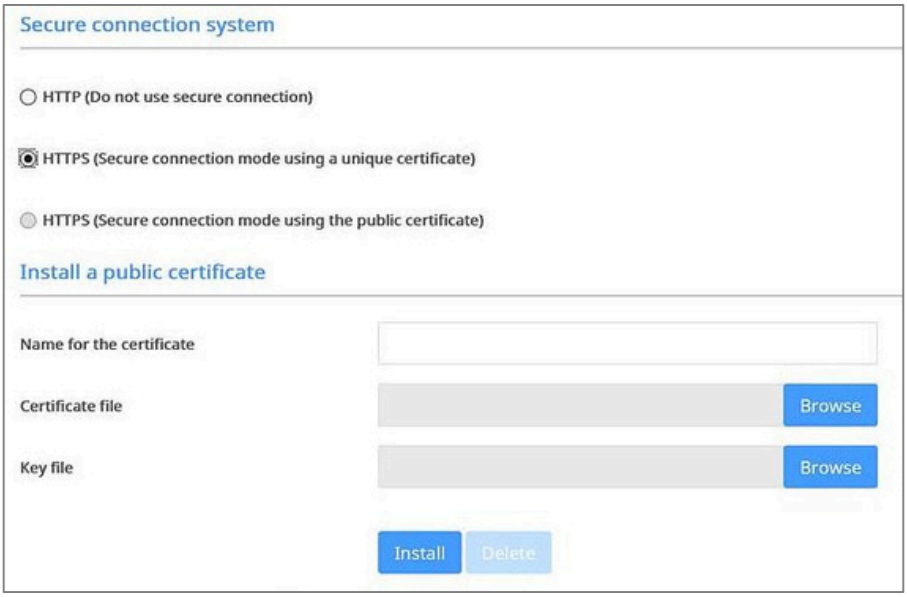
Savukārt šifrēšanas autentificēšana šifrē datus, izmantojot šifrēšanas funkciju, kas pēc tam tiek salīdzināta ar ierīcē esošajiem šifrētajiem akreditācijas datiem. Tādējādi šifrēšanas autentifikācija pastiprina drošību, jo tīklā netiek sūtīti faktiskie lietotājvārdi un paroles.

Hanwha Vision produkti atbalsta šifrētas paroles un nenodrošina pamata autentifikāciju. Tomēr to pašu nevar teikt par katru klientu, kas pieslēdzas ierīcei. Tāpēc ir svarīgi noteikt to iespējas, lai nodrošinātu, ka visi klienti a) darbojas un b) neatgriežas pie skaidra teksta vai base64 paroles.

4.2. SSL šifrēšana

SSL ir lieliska metode, lai nodrošinātu, ka lietotāja akreditācijas dati un dati tiek nosūtīti uz tiem paredzētajiem galamērķiem. Šī vienkāršā un rentablā metode vēl vairāk uzlabo ierīces drošību. Iebūvētie sertifikāti ļauj SSL šifrēšanu izveidot un izmantot dažu sekunžu laikā. SSL sertifikātu var arī iegādāties no komerciālas sertifikātu iestādes vai izsniegt no korporatīvajām struktūrām, lai nodrošinātu vēl lielāku drošību un izvairītos no sertifikāta drošības ziņojuma, kad tiek saņemts piekļuves ziņojums.
Lai gan SSL drošība ir lielisks veids, kā nostiprināt saziņas kanālu potenciāli nedrošā tīklā vai mākonī, noskaidrojiet, kuri kanāli ir šifrējami un ir atbalstīti. Tas ietver kameras savienojumu ar NVR/VMS un VMS savienojumu ar klientu. SSL šifrēšana jāizmanto arī, sūtot e-pasta paziņojumus, izmantojot SMTP protokolu, lai novērstu akreditācijas datu nosūtīšanu atklātā tekstā. Pārliecinieties, ka jūsu SMTP serveris atbalsta SSL/TLS, un pārbaudiet, kāds ports tiek izmantots.

Konfigurēšanas opcijas ļauj izvēlēties unikālu (iebūvētu) vai publisku sertifikātu, kā arī uzstādīt un nosaukt sertifikāta un atslēgas failu. Ja tiek mainītas HTTPS opcijas, kamera tiks pārstartēta un pēc tam tiks atļauta tikai šifrēta HTTPS saziņa, izmantojot HTTPS portu (sk. 4. attēlu)



4. attēls. SSL šifrēšanas konfigurācija

4.3. MĀKOŅKRĀTUVES MINIMĀLA IZMANTOŠANA

Mākoņpakalpojuma izmantošana sistēmas ierakstīšanai vai skatīšanai ne tikai prasa lielu joslas platumu, bet arī var radīt drošības problēmas. Kad mākonis izveido savienojumu ar ierīci, tas nosūta pieteikšanās informāciju. Ja šī informācija tiktu pārtverta vai tiktu izmantots "cilvēks pa vidu" (MITM) uzbrukums, akreditācijas datus varētu atšifrēt vai atveidot, tādējādi nodrošinot neatļautu piekļuvi. Turklāt ne visi mākoņpakalpojumi atbalsta SSL šifrēšanu vai pat digitāla autentifikāciju.

5.1. FIZISKĀ TĪKLA NOŠĶIRŠANA

Viens no izplatītākajiem un efektīvākajiem paņēmieniem, kā palielināt drošības tīkla drošību, ir fiziski atdalīt kameras un ierakstīšanas ierīces no uzņēmuma tīkla. Tas neļauj uzbrucējiem iegūt piekļuvi, jo piekļuves nav. Daudziem NVR ir vairākas tīkla saskarnes, kas ļauj ierakstīt no vienas un nodrošināt piekļuvi darba stacijai no otras. Šis paņēmiens samazina ārēji eksponētu ierīču skaitu, kurām nepieciešama pastiprināta drošības kontrole.

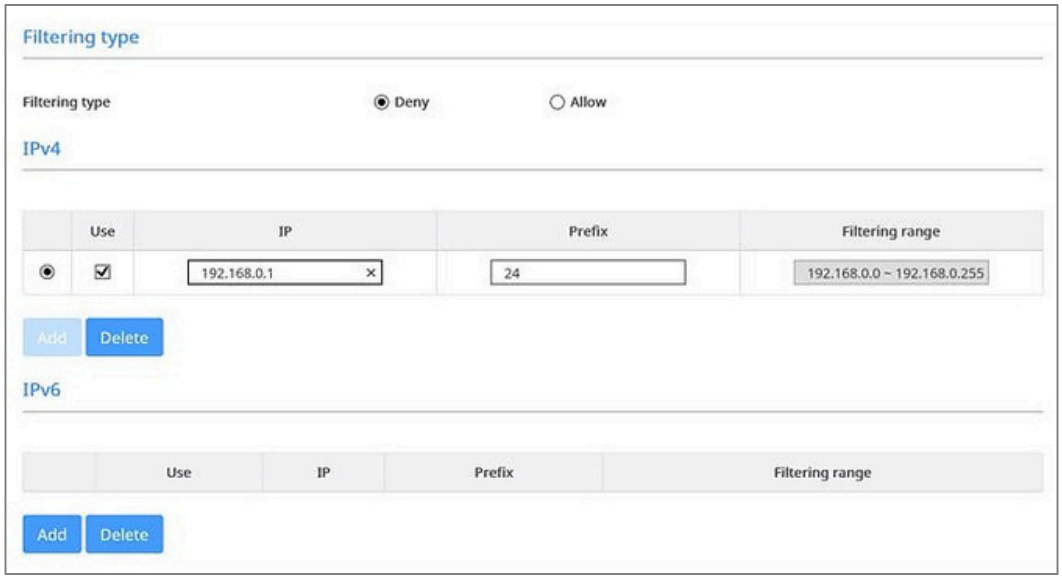
5.2. VLAN

Virtuālo LAN (VLAN) ieteicams izmantot, lai drošības tīklu nodalītu no korporatīvā tīkla, ja netiek izmantots atsevišķs tīkls. VLAN darbojas tīkla komutatoros un parasti sadala datplūsmu, pamatojoties uz komutatora pieslēgvietām. Tas ļauj ugunsmūriem aizsargāt drošības ierīces no citām tīkla ierīcēm. Ja nepieciešama piekļuve konkrētām ierīcēm, var izveidot ugunsmūra noteikumus vai pievienot VLAN ierīci.

5.3. IP FILTRĒŠANA

IP filtrēšana ir metode, ar kuras palīdzību var skaidri norādīt, kam ir atļauts piekļūt tīkla ierīcei, vai, gluži pretēji, kam piekļuve ierīcei ir liegta. Var norādīt IP adresi vai diapazonu/apakštīklu. Tādējādi var nodrošināt, ka ierīcei var piekļūt tikai pareizās personas, pamatojoties uz viņu datora IP adresēm, un piekļuve tiek liegta, ja tiek mēģināts piekļūt no vietējā tīkla vai interneta. Hanwha Vision ierīces ļauj ievadīt lPv4 un lPv6 IP adreses un prefiksus, lai liegtu vai atļautu piekļuvi. Pirms apstiprināšanas un piemērošanas tiks parādīts filtrējamais diapazons, lai apstiprinātu IP un prefiksu.

Pārliecinieties, ka tas ir pārbaudīts pirms piemērošanas, pretējā gadījumā piekļuve var tikt liegta. Katram lPv4 un lPv6 var pievienot līdz 10 ierakstiem (5. attēls).



5. attēls. IP šifrēšanas konfigurācija

5.4. VPN

Labākā prakse, lai savienotu attālinātas atrašanās vietas, piemēram, vairākus birojus vai attālinātus darbiniekus, ir izmantot VPN risinājumu. Tādējādi tiek izveidots drošs, šifrēts kanāls, novēršot informācijas, piemēram, lietotājvārdu un paroļu, noplūdes iespēju. VPN risinājums var ietvert īpašu aparatūru, piemēram, VPN maršrutētāju, un/vai programmatūras VPN, kas darbojas klienta datorā.

5.5. NOKLUSĒJUMA PORTU MAIŅA

Mūsdienu savienotajā pasaulē daudzas ierīces ir savienotas ar internetu (tīši vai netīši), un hakeri izmanto daudzus pakalpojumus, lai veiktu skenēšanu un meklētu šīs ierīces. Viens no vienkāršiem veidiem, kā kavēt šo skeneru, kā arī skriptu bērnu, "drive-by" uzbrukumu un netīšas piekļuves iespējamību, ir mainīt tīkla ierīču porti no labi zināmajiem noklusējuma iestatījumiem, kas ir viegli pieejami tiešsaistē, uz lielākiem portu numuriem pēc jūsu izvēles. Īpaši svarīgs ir HTTP tīmekļa ports, kas lielākajā daļā ierīču pēc noklusējuma ir 80 porti, lai nodrošinātu piekļuvi, izmantojot tīmekļa pārlūkprogrammu. Piemēram, mainot šo portu uz 8000, ir nepieciešams veikt papildu darbību, kad ievadot adresi tīmekļa pārlūkprogrammā, kas bieži vien aizsargā no vienkārša skenera vai kāda cita personas, kas manuāli ievada adresi tīmekļa pārlūkprogrammā

5.6. NEIZMANTOTO PORTU, PAKALPOJUMU UN PROTOKOLU ATSPĒJOŠANA

Ņemot vērā, ka daudzas drošības ierīces ir pilnvērtīgi datori ar modernām operētājsistēmām, Hanwha Vision ir izvēlējusies izmantot pēc pasūtījuma izstrādātas, samazinātas Linux operētājsistēmas, kurās visi neizmantojamie pakalpojumi ir noņemti vai atspējoti. Daudzi citi ražotāji atstāj šos pakalpojumus pieejamus atkļūdošanas nolūkā vai arī tāpēc, ka tiem trūkst stingras drošības izpratnes un/vai nostājas. Vairākos nesenos incidentos, kad tika uzlauztas citu ražotāju ierīces, uzbrucēji iekļuva ierīcē, izmantojot telnet, kas nodrošina pilnu komandrindas piekļuvi visiem failiem un pakalpojumiem. Uz Windows bāzētās ierakstīšanas platformās darbojas virkne pakalpojumu, papildus tam, ka ir nepieciešami pastāvīgi drošības atjauninājumi un labojumi, kas prasa laiku, izsekošanu un piekļuvi internetam.

Hanwha Vision ierīces izmanto dažādus protokolus, kas nodrošina noderīgas funkcijas. Tomēr ir ieteicams atslēgt visus pakalpojumus, kas nav nepieciešami lietojumprogrammai. Tas varētu ietvert multiraides, dinamisko DNS (DDNS), pakalpojuma kvalitāti (QoS), Bonjour, Universal Plug and Play (UPnP) atklāšanu un portu pāradresēšanu, saites vietējo adresi, failu pārsūtīšanas protokolu (FTP), tīkla atmiņas ierīci (NAS) un e-pasta paziņojumus. Kā minēts iepriekš, unikālu pilnvaru ieviešana un FTP, NAS un e-pasta tiesību ierobežošana ir arī lielisks veids, kā vēl vairāk uzlabot drošību.

Automātiskās IP konfigurēšanas protokoli ir iespējoti pēc noklusējuma, savukārt visi pārējie uzskaitītie pakalpojumi ir atspējoti.

5.7. RTSP

Daudzi VMS straumē video, izmantojot RTSP protokolu. Hanwha Vision kameras nodrošina iespēju atļaut RTSP video savienojumus bez autentifikācijas. Tas var būt noderīgi, sūtot plūsmas internetā publiskai apskatei, lai nodrošinātu, ka akreditācijas dati netiek atklāti, vai trešo pušu integrācijai, ja autentifikācija netiek atbalstīta. Hanwha Vision kamerām šo funkciju var viegli aktivizēt no kameras lietotāja saskarnes izvietošanas laikā, ja nepieciešams. Tomēr drošības apsvērumu dēļ ir ieteicams pieprasīt autentifikāciju visai video plūsmai. Ja ir nepieciešama publiska skatīšanās, trešās puses pakalpojumi var ievadīt autentificēto plūsmu un nodrošināt publisku piekļuvi, izmantojot citu portālu, izolējot kameru no tiešas publiskas piekļuves. Hanwha Vision kameras neatver paroles, izmantojot RTSP protokolu, jo pēc noklusējuma atbalsta digest autentifikāciju, kā arī HTTP protokolu.

Trīs no visbiežāk izmantotajām hakeru uzbrukumu metodēm ir brute-force, pakalpojuma atteikums (DoS) un bufera pārpildīšana. Katra no šīm metodēm ir izrādījusies efektīva uzbrukumos, tāpēc, lai aizsargātu ierīces un tīklus no nesankcionētas piekļuves, tām ir jāpievērš pienācīga uzmanība. Hanwha Techwin kamerās ir iekļautas divas metodes, kas ir izrādījušās ļoti efektīvas šī mērķa sasniegšanai.

6.1. LIETOTĀJA KONTA BLOĶĒŠANA

Hakeri sistemātiski pārbauda visas iespējamās paroles un paroles frāzes, līdz atrod pareizo. Ja šis uzbrukums tiek pieļauts, parole pēc kāda laika tiek izņemta. Hanwha Techwin ierīces bloķē brutālā spēka uzbrukumu, nepieļaujot 5 vai vairāk pieteikšanās mēģinājumus 30 sekunžu laikā, lai uzlabotu tās drošību. Lai novērstu pakalpojuma atteikumu, kamēr tiek bloķēta paroles ievadīšana, tiek saglabāts arī autorizētā lietotāja esošais savienojums.

6. attēls. Paroles ievades bloks

6.2. BUFERA PĀRPLŪDES AIZSARDZĪBA

Vēl viens izplatīts uzbrukuma vektors ir hakeri, kas ierīcei nodod rūpīgi sagatavotas komandas, mēģinot izpaust informāciju vai nosūtīt komandas tieši citiem pamatā esošajiem pakalpojumiem, piemēram, datubāzēm vai failu sistēmām. Bieži vien šajās komandās tiek izmantota datu analizatora vai datubāzes vājā vieta vai tiek bojāta saskarne, ļaujot nosūtīt komandas tieši datubāzes serverim, operētājsistēmai vai failu sistēmai. Hanwha Vision ierīces filtrē komandas pirms to nodošanas tīmekļa serverim vai datubāzei, novēršot uz bufera pārpildīšanu un tiešu uzlaušanu balstītus uzbrukumus, padarot pamatā esošos pamatpakalpojumus hakeriem nepieejamus.

6.3. IERĪCES IZVIETOJUMS UN FIZISKĀ PIEKĻUVE

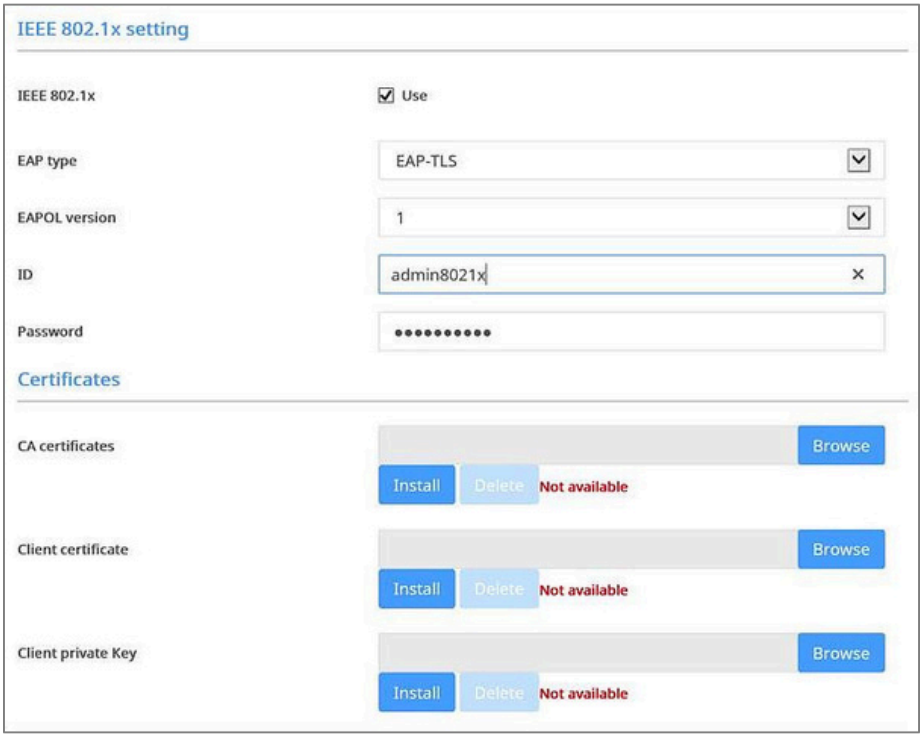
Kameras jāuzstāda tā, lai tās nevarētu viegli aizsniegt, novirzīt vai atvienot, vēlams, ar piemērotu korpusu, lai tām nevarētu fiziski piekļūt. Tīkla un strāvas kabeļiem jānovada caur cauruļvadiem vai aiz/caur sienām un griestiem, lai kabeļus nevarētu atvienot vai pārtvert. Lai nodrošinātu vislabāko fizisko drošību, apsveriet vandal kupolu modeļus. Fiziska piekļuve jebkurai tīkla ierīces drošībai ir ārkārtīgi svarīga. Izmantojot fizisku piekļuvi, lielāko daļu ierīču var iestatīt pēc noklusējuma, tādējādi ļaujot neautorizētām personām konfigurēt jaunus iestatījumus. Saskaņā ar padziļinātās aizsardzības drošības modeli ir ļoti svarīgi, lai tīkla ierīces būtu uzstādītas aiz slēdzenes un atslēgas, vēlams ar piekļuves kontroli un/vai videonovērošanu. Tas nodrošina vairāku līmeņu drošību, nepaļaujoties tikai uz vienu mehānismu.

6.4. NEPĀRTRAUKTAS IERAKSTĪŠANAS NODROŠINĀŠANA

Laupīšanas laikā zagļi bieži vien nozog vai iznīcina ierakstīšanas ierīci vai serveri, mēģinot iznīcināt video pierādījumus. Viena no metodēm, kā pret to cīnīties, ir izmantot SD kartes, kas ierakstītas katrā no jūsu kamerām. Lai gan ierakstu saglabāšanas periods būs īsāks, tas nodrošinās dublēto ierakstu iespējas. Ierakstīšanu SD kartē var izmantot arī NVR/VMS atteices un tīša vai nejauša tīkla darbības pārtraukuma gadījumā, ja kamerai joprojām ir strāva. Konfigurēšanas opcijas ietver SD kartes funkciju ieslēgšanu/izslēgšanu, nepārtrauktu/pasākumu ierakstīšanu pilnā/I-Frame/vienreizēju, ierakstīšanas ilgumu pirms un pēc notikuma, ieraksta faila veidu (AVI/STW), pārrakstīšanu, automātisko dzēšanu/ilgumu, parasto ierakstīšanas grafiku un SD kartes failu sistēmu. Ierakstīšanai var izvēlēties jebkuru profilu/kodeksu. SD karti var pārformātēt, ja nepieciešams, tomēr tukša SD karte, kas ir ievietota, tiks automātiski konfigurēta. SD kartes vietā var konfigurēt arī NAS vai kā primāro ierakstīšanas ierīci ar SD karti kā papildu rezerves ierakstīšanas datu nesēju. NAS ierakstīšanai ir tādas pašas konfigurācijas opcijas, pievienojot IP adresi, lietotāja ID, paroli un noklusējuma mapi.

6.5. 802.1X UZ SERTIFIKĀTU BALSTĪTA PIEKĻUVES KONTROLE

Daudzās ēkās tīkla ligzdas var būt pieejamas vai arī var atvienot kameru vai bojāt kabeli, lai piekļūtu Ethernet tīkla infrastruktūrai. 802.1x standarts nodrošina uz pieslēgvietām balstītu tīkla piekļuves kontroli, kas pieprasa, lai katrā pieslēgtajā ierīcē tiktu instalēts identificējošs sertifikāts, kas ļauj piekļūt aizsargātajam tīklam. Tādējādi, ja uzbrucējs pieslēgs neatļautu ierīci tīklam, tai piekļuve tiks liegta. Wisenet ierīču pārvaldnieku var izmantot, lai viegli aktivizētu 802.1x, kā arī ieviestu sertifikātus no centralizētas atrašanās vietas bez nepieciešamības veikt konfigurācijas katras kameras saskarnē. Konfigurēšanas opcijas ietver EAP tipa, EAPOL versijas, lietotāja ID un paroles, kā arī sertifikātu / atslēgu uzstādīšanas izvēli.



7. attēls. Sertifikātu uzstādīšanas ekrāns

6.6. JAUDA

Ar UPS var nodrošināt, ka tīkla ierīces netiek izslēgtas un tiek novērsti bojājumi, ko rada pārspriegumi strāvas padeves traucējumu, vadāmu atslēgumu, brūnogriezumu un nejaušu vai ļaunprātīgu atslēgumu laikā. Ja UPS ir pieslēgts tīklam pārvaldības nolūkā, pārliecinieties, ka tas ir pienācīgi nodrošināts un ir instalēti drošības atjauninājumi. Ir bijuši gadījumi, kad uzbrucēji piekļūst drošam tīklam, izmantojot palīgierīces, piemēram, UPS, kas bija pieslēgts LAN vai internetam, lai veiktu uzraudzību. Daudzām IP kamerām var būt arī divi barošanas avoti - PoE un zemsprieguma 12vDC/24vAC atkarībā no modeļa, lai nodrošinātu dublēto barošanu gadījumā, ja tiek pārsniegts PoE barošanas budžets.
Lielākajai daļai tīkla komutatoru var noteikt prioritāti, lai norādītu, kāda veida ierīcei (tālruņi, kameras, WAP u. c.) vai kuras pieslēgvietas ir svarīgākas, ja trūkst enerģijas.

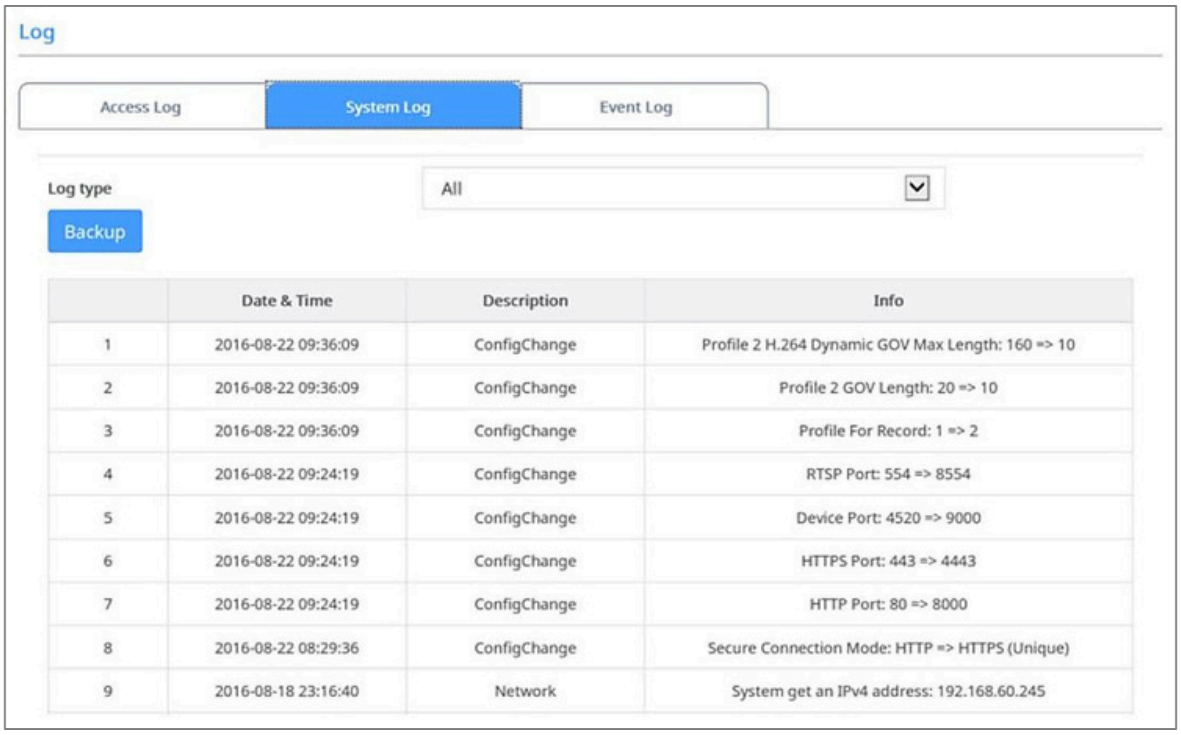
6.7. TĪKLA ADMINISTRĒŠANA

Papildus izvietošanai tīkla administratoriem pastāvīgi jāveic vairāki uzdevumi, lai nodrošinātu nepārtrauktu kameru un citu ierīču drošību. Starp vissvarīgākajiem uzdevumiem ir visu izmaiņu pārskatīšana, konsekventu un apstiprinātu konfigurāciju izstrāde un nodrošināšana, programmatūras atjauninājumu veikšana un programmatūras atbilstības nodrošināšana organizācijas drošības standartiem. Kā šeit izklāstīts, Hanwha Techwin atzīst, ka katram no šiem aspektiem ir izšķiroša nozīme spēcīgas vispārējas stratēģijas izveidē, lai bloķētu ierīces un aizsargātu tīklus no hakeriem.

6.7. IERĪCES ŽURNĀLU PĀRBAUDE

Ņemot vērā, ka Hanwha Vision kameras reģistrē visas ierīces iestatījumu izmaiņas, ir svarīgi pārbaudīt žurnālus, lai noteiktu, kādas izmaiņas ir veiktas un kas tās ir veicis. Lai būtu iespējams viegli atjaunot iestatījumus, lielākajā daļā žurnāla ierakstu ir iekļauti gan iepriekšējie, gan jaunie iestatījumi, un žurnālos tiek saglabātas rūpnīcas noklusējuma iestatījumu laikā. Saglabātos žurnālus var izmantot maršruta analīzei un izsekošanai atpakaļ, ja ir noticis pārkāpums. Wisenet ierīču pārvaldnieku var izmantot, lai viegli lejupielādētu žurnālus no vairākām ierīcēm vienlaicīgi. Ja iestatījumus nav iespējams pārbaudīt, var būt nepieciešams veikt rūpnīcas noklusējuma iestatījumus, lai nodrošinātu, ka ir ieviesti zināmi labi iestatījumi.

Hanwha Vision kamerām to var izdarīt, vienkārši piecas sekundes turot ieslēgtu rūpnīcas noklusējuma pogu, kamēr kamera ir ieslēgta. Pēc kameras noklusējuma iestatīšanas ir svarīgi konfigurēt IP adresi un mainīt noklusējuma administratora paroli. Rūpnīcas noklusējuma iestatījumus var izpildīt, saglabājot visus izvēlnes "IP & Port" un "Network" iestatījumus.



8. attēls. Konfigurācijas izmaiņu vēsture sistēmas žurnālos

6.9. REGULĀRA PROGRAMMAPARATŪRAS ATJAUNINĀŠANA

Hakeri nenogurstoši strādā, lai atklātu un izmantotu programmatūras ievainojamības, jo īpaši novecojušās versijas, kas nav atjauninātas, lai uzlabotu drošību. Kad ievainojamība ir u-iseNeT, tā bieži vien tiek ātri izplatīta tiešsaistē, paverot iespēju vairākiem cilvēkiem viegli piekļūt jebkurai ierīcei ar vecāku programmaparatūras versiju - un līdz ar to arī pašam tīklam. Programmatūras nodrošinātāji to apzinās un nepārtraukti izdod atjauninājumus, lai nodrošinātu uzlabojumus un/vai labojumus, kas aizver šīs durvis un aizsargā lietotājus no nesankcionētas piekļuves.

Katras Hanwha Vision ierīces programmaparatūrā ir iekļauts atjauninājumu saraksts, uz kuru administratori var atsaukties, lai pārliecinātos, ka tiek izmantota jaunākā versija.

Pirms sistēmas izvietošanas ir ieteicams atjaunināt programmaparatūru un regulāri atjaunināt tās versijas. Daudzi uzstādītāji izvēlas atjaunināt programmaparatūru, piešķirt IP adreses un iestatīt administratora paroles uz stenda pirms izvietošanas. Izmantojot rīku Wisenet Device Manager, var viegli pārbaudīt visu ierīču programmaparatūras versiju un atjaunināto statusu, un programmaparatūru var lejupielādēt un instalēt tikai ar dažiem vienkāršiem klikšķiem.

6.10. ŠIFRĒTA PROGRAMMAPARATŪRA

Lielākā daļa drošības ierīču ražotāju piedāvā programmaparatūru, lai lietotāji varētu pievienot funkcijas, labot kļūdas un atjaunināt drošību. Šiem uzlabojumiem paredzētā programmaparatūra var būt arī hakeru mērķis. Programmatūrā ir vairāk svarīgas informācijas, nekā mēs domājam. Piemēram, tajā ir algoritmi lietotāju kontu identificēšanai, šifrēšanas algoritmi un atslēgas informācija, ko izmanto sensitīvas informācijas šifrēšanai, operētājsistēmas faili vai svarīgi tīmekļa pakalpojumu URL, un, ja tie tiek atklāti, pastāv arī vājību atklāšanas iespēja, kas var iekļūt programmaparatūras aizmugurē. Ja tiek izplatīta bojāta programmaparatūra, kas ietver backdoor, hakeris var pārņemt kontroli pār ierīci un izmantot to kā kontrolpunktu citiem perifēro sistēmu uzbrukumiem.

Lielākajai daļai iegulto ierīču, tostarp tīkla drošības ierīcēm, nav īpašu aizsargmehānismu programmaparatūras drošībai. Tomēr Hanwha Techwin izplata šifrētu programmaparatūru, izmantojot nozarē ieteikto šifrēšanas algoritmu, lai nodrošinātu drošību un drošus atjauninājumus. Tāpēc, ja tiek izdota jauna programmaparatūra, droši atjauniniet to ar jaunāko programmaparatūru.

6.11. VIDEO FORMĀTI

Lielākā daļa drošības iekārtu atbalsta nozares standarta, atvērtos video formātus, kā arī patentētus video formātus. Šķiet, ka atvērtais video formāts var šķist ideāls, jo lietotāji var vienkārši atvērt video ar savu iecienītāko multivides atskaņotāju. Tomēr drošības lietojumprogrammās ir nepieciešams formāts, ko nevar rediģēt, mainīt vai manipulēt ar to. Tas ir būtiski, jo, lejupielādējot videoklipu, ir jābūt mehānismam, kas ļauj autentificēt videoklipu un nodrošināt, ka ar to nav manipulēts.

Hanwha Vision nodrošina ūdenszīmes funkciju, kas var pārbaudīt, vai video ir viltots, saglabājot video hash informāciju katram kadram, kad tas tiek saglabāts SEC formātā NVR / VMS. Ja ir iestatīta parole, tā tiek saglabāta šifrētā SEC formātā, tāpēc jūsu personisko informāciju var aizsargāt pat tad, ja video fails tiek nopludināts. SEC formātā atskaņošanai nepieciešams īpašs atskaņotājs, kas automātiski tiek iekļauts dublēšanas laikā. Hanwha Vision VMS, SSM atbalsta ne tikai ūdenszīmes funkciju, bet arī digitālo parakstu, un var parakstīt un pārbaudīt video viltojumu, izmantojot visa video attēla hash informāciju. Ūdenszīmes un digitālā paraksta apstiprināšana ir iespējama, izmantojot dublējuma pārlūku.

Tā spēj veidot dublējumu AVI faila formātā, izmantojot ierakstīšanas ierīču tīmekļa pārlūkprogrammu. Ņemot vērā, ka video fails ir atvērtā video formātā, to var atskaņot ar universālo multivides atskaņotāju. Hanwha Vision IP kameras var saglabāt videoklipus STW faila formātā un eksportēt tos, izmantojot tīmekļa pārlūku. To var atskaņot un konvertēt AVI faila formātā, izmantojot autonomo SD kartes atskaņotāju.

6.12. ATVĒRTĀS PLATFORMAS LIETOTNES

Daudzas Hanwha Vision kameras ļauj uzstādīt trešo pušu lietojumprogrammas, lai uzlabotu to funkcijas, piemēram, nodrošinot numura zīmju atpazīšanu, mazumtirdzniecības biznesa izlūkošanu, cilvēku skaitīšanu un citas. Lietojot lietojumprogrammas kamerās, ir svarīgi zināt, kuras no tām ir instalētas, kā arī programmatūras paketes avotu.

Instalēšanas laikā Hanwha Vision kameras informē par nepieciešamajām lietotnes atļaujām; uzmanīgi izlasiet šo informāciju un pārliecinieties, vai dati tiks nosūtīti uz kādu citu vietu. Ja lietotni nevar pārbaudīt vai ja tās mērķis nav zināms, nekavējoties pārtrauciet instalēšanu, atinstalējiet lietotni un iegūstiet to no uzticama partnera, kas to nodrošina. Konfigurēšanas opcijas ietver automātiskās palaišanas iestatīšanu, prioritātes līmeni, lietotņu palaišanu/apturēšanu, lietotņu instalēšanu/ atinstalēšanu un lietotnes tīmekļa lapas izpildi.

7. Secinājumi

Šodienas savienotajā pasaulē realitāte ir tāda, ka indivīdi un grupas turpinās mēģinājumus identificēt un izmantot ievainojamības, lai pārkāptu tīkla drošību. Un, lai gan mēs gūstam labumu no pieaugošā ierīču skaita, kas ir pieejamas šajos tīklos, ērtībām, realitāte ir tāda, ka šīs ierīces tikai palielina nesankcionētas piekļuves tīklam iespējamību. Tāpēc ir ļoti svarīgi, lai visas šīs ierīces tiktu aizsargātas, lai tās nekļūtu par atvērtām durvīm hakeriem. Izmantojot šo paraugpraksi, var ne tikai novērst to, ka tīkla video ierīces un sistēmas kalpo par piekļuves punktiem, bet arī nodrošināt šīs kritiski svarīgās funkcijas integritāti un nepārtrauktu darbību, tādējādi nodrošinot pastāvīgu cilvēku un aktīvu drošību un aizsardzību. Turklāt daudzi no šiem pasākumiem ir piemērojami arī citām ierīcēm un sistēmām. Tāpēc šī paraugprakse kalpo kā prasība organizācijām, kas atzīst savu tīklu drošības nozīmi un nopietni domā par to drošību.

Tāpēc šī paraugprakse kalpo kā sarunu sākšanas līdzeklis organizācijām, kas apzinās savu tīklu drošības nozīmi un nopietni domā par to. Atklāts un informēts dialogs starp galalietotāju, IT nodaļu, uzstādītāju un sistēmu integratoru ir galvenais, lai atrastu labāko risinājumu, kas atbilst konkrētās organizācijas drošības vajadzībām. Hanwha Vision pārbauda produktu drošību un diagnosticē ievainojamību jau izstrādes posmā, izmantojot savu drošības komandu un specializētu iestādi. Lai nodrošinātu uzticamu drošību, visiem produktiem tiek piemērotas stingras politikas, piemēram, lietotāja autentifikācija, datubāzes un programmaparatūras šifrēšana, aizmugurējo durvju likvidēšana un stingra paroles identifikācija un noteikumi.

WISENET

ALTAS IT SIA - oficiālais Hanwha Vision distributors Latvijā

Brīvības gatve 221-1, Rīga, LV-1039
+371 66 100 650
info@altas.lv
https://www.altas.lv/videonoverosana/hanwha-vision

Hanwha Vision