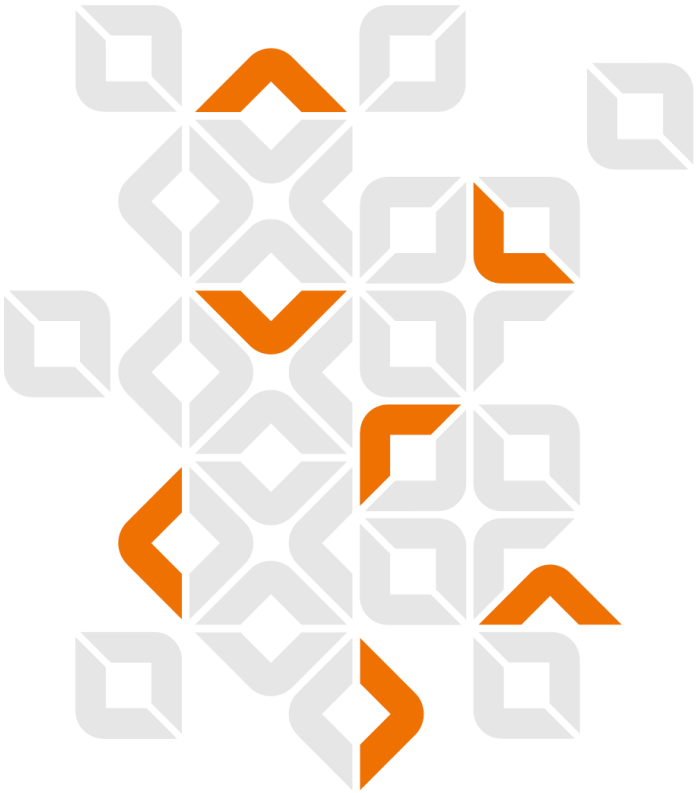
ALVERAD
TECHNOLOGY FOCUS

Hazai kamerák az interneten –

Ki figyeli az őrzőket?

Tanulmány a hazai, internet felől elérhetővé tett kamerák használatával és kockázataival kapcsolatban



Készítette: Kocsis Tamás

Kiadás dátuma: 2020.12.17

Dokumentum verzió: 1.3

SECURITY TESTING LABORATORY
MAKING THE WORLD SAFER

Tartalom

Bevezető

A webkamerák és egyéb, megfigyelésre alkalmas berendezések, mint például az IP-alapú biztonsági kamerák és baba monitorok, az IoT világához tartozó eszközöknek számítanak. Az *Internet of Things* korában kis túlzással minden eszközt ide tartozónak érthetünk, amely kapcsolódik az internethez, vagy elérhető az internet irányából.

Számos szakcikk és tanulmány foglalkozik a kamerák és megfigyelő eszközök internet felőli elérhetőségének kérdésével, a szakemberek évek óta hívják fel a figyelmet arra, hogy ilyen készülékeket megfelelő védelem hiányában az internet felől elérhetővé tenni nem biztonságos.

A kamerák (akárcsak a többi IoT eszköz) számos biztonsági hiányossággal és sérülékenységgel rendelkezhetnek. A sérülékenységek vagy a gyenge biztonsági beállítások lehetőséget adhatnak a támadónak, hogy jogosulatlanul hozzáférjen a kamerához, átvegye a kamera irányítását (például kamera mozgatás), kommunikációt kezdeményezzen a kamera mikrofonján keresztül, illetve természetesen a kamera által rögzített képhez is hozzáférhet.

Még 2019 decemberében jelentetett meg a CNN egy cikket, amelyben beszámolnak egy meglehetősen ijesztő történetről, ahol egy idegen kezdeményezett kommunikációt a gyermeket figyelő biztonsági kamera hangszóróján keresztül, azt állítva, hogy ő a Mikulás, és szeretné, ha barátok lennének[1]. Ugyanez a cikk számol be egy másik eseményről is, amikor egy nőt ébresztett fel egy idegen a kamera hangszóróján keresztül, továbbá egy rasszista zaklatóról, aki feltehetőleg már napok óta figyelt egy családot a kamerán keresztül. A kamera gyártója kivizsgálta ezeket az eseteket és megállapította, hogy nem egy sérülékenység, hanem a kamerák gyenge biztonsági beállítása miatt volt lehetőségük az elkövetőknek a tulajdonosokat és családjukat megfigyelni, illetve zaklatni.

A *hacked.camera* oldal 2020 augusztusi körképében 3.7 millió sérülékeny kamerával kapcsolatban adott ki figyelmeztetést, azonban ez csak a jéghegy csúcsa lehet, mivel a figyelmeztetés főleg a Shenzhen Hcip Vision-alapú, illetve CS2 Network P2P szolgáltatást tartalmazó eszközöket érintette. A XiongMai (XM) eszközeivel kapcsolatban (az Aliexpressen kapható „filléres" kamerák közül sok az XM technológiájára épül) még 2018-ban jelent meg, hogy az XM P2P felhőszolgáltatáson keresztül váltak kompromittálhatóvá.

A sérülékenységek felismerését nehezíti az a tény is, hogy nagyon sok gyártó OEM licenszeli a technológiát, azaz más gyártó eszközeit a saját márkája alatt (vagy éppen teljesen névtelenül) értékesíti, így az eszközök azonosítása is meglehetősen nehézkes. Például a Shenzhen Hcip Vision, vagy akár a NetSuveillance technológiát akár sokszáz gyártó is használhatja, azaz a sérülékeny eszközöket gyakran nagyon nehéz gyártóhoz, márkához és típushoz kötni.

Jelen tanulmány nemcsak a „klasszikus" sérülékenységekkel foglalkozik, hanem azzal a jelenséggel is, amely egyértelműen a biztonságtudatosság hiányához, illetve az ember és a technológia közti olló szélesre nyitásához köthető: olyan kamerákkal, amelyek elérhetők az internet felől, és bárki képes hozzájuk csatlakozni, illetve betekinteni az általuk rögzített felvételekbe.

[1] *https://edition.cnn.com/2019/12/12/tech/ring-security-camera-hacker-harassed-girl-trnd/index.html*

Kamerák az interneten

Lehetséges okok

Felmerül a kérdés, vajon hogyan válik egy megfigyelő kamera elérhetővé és betekinthetővé az internet felől? Erre többféle lehetséges válasz is akad.

Előfordulhatnak olyan eszközök, amelyeket üzemszerű célok miatt és szándékosan tesznek elérhetővé és betekinthetővé. Ilyenek lehetnek például a különféle turisztikai vagy látványossági célból, bárki számára elérhető és betekinthető kamerák, amelyek valamilyen érdekes, figyelemfelkeltő és szemet gyönyörködtető képeket közvetítenek. Ebben az esetben pontosan az a cél, hogy bárki csatlakozhasson, és láthassa a kamera által közvetített képeket vagy videófolyamot.

A következő lehetőség, hogy valamilyen elvárás miatt szándékosan, de a biztonsági szempontokat figyelmen kívül hagyva teszik elérhetővé és betekinthetővé a kamerát. Erre legtöbbször azért kerülhet sor, mert a *rendelkezésre állás* elvárása (bárhonnan, bármikor ellenőrizhető legyen) felülírja a *bizalmasság* (csak arra jogosult férhessen hozzá) elvárását. Ilyen esetekben a kamera távoli hozzáférése tudatosan engedélyezett, és általában megpróbálják azt biztonságosan beállítani, például felhasználónévhez és jelszóhoz kötni a hozzáférést, azonban egyéb hiányosságok miatt (sérülékenység, statikus képek engedélyezése, hibás konfiguráció, alapértelmezett jelszavak, rejtett vagy nem ismert hozzáférések, stb.) jogosulatlan személyek is hozzáférhetnek az eszközökhöz, és a közvetített képekhez vagy videófolyamokhoz.

A felhasználó hiányos szakmai ismerete és a biztonságtudatosság hiánya is közrejátszhat abban, hogy jogosulatlan személyek is betekinthetnek a kameraképekbe vagy a videófolyamokba. Az ember és a technológia közötti olló szárai mára már olyan szélesre nyíltak, hogy a felhasználók sokszor nincsenek tisztában az eszközök működésével, képességeivel és funkcióival. A legjobb példa erre az UPnP használata. Az UPnP egy kényelmi funkció, amely segítségével a kamera, illetve más eszközök emberi beavatkozás és kontroll nélkül egyeztethetik, hogy milyen kommunikációs portra van szükség a működésükhöz. Ez azt jelenti, hogy a kamera (vagy más eszköz) önállóan megkéri a router vagy tűzfal eszközt arra, hogy engedélyezzen számára bizonyos eléréseket, illetve tegye lehetővé, hogy őt magát az internet felől el lehessen érni. Látható, hogy ha a felhasználó nincs tisztában a saját routerének beállításával, illetve azzal, hogy a kamera kérheti, hogy a router tegye az internet felől elérhetővé a videófolyamot, akkor az eszközök és funkciók nem ismerete elvezethet odáig, hogy jogosulatlan személyek tekinthetnek bele. Tapasztalatunk szerint az otthoni kamerák esetében ez az illetéktelen hozzáférések leggyakoribb oka.

Még akkor is bekövetkezhet a jogosulatlan hozzáférés, ha a felhasználó vagy üzemeltető megpróbálta a lehető legtöbbet megtenni azért, hogy biztosítsa a bizalmasságot. Ha egy eszköz közvetlenül elérhető az internet felől, akkor az esetleges eszközsérülékenységek kihasználhatóvá válhatnak és hiába állított be a felhasználó jelszavas védelmet, cserélte le az alapértelmezett jelszavakat, vagy tiltotta le az UPnP-t és statikus képek betekintését, az internet lehetőséget biztosít a támadónak, hogy a sérülékenységen keresztül megkerülje a beállított védelmi intézkedéseket.

A leggyakrabban a különféle webes protokollokon (HTTP, HTTPS), illetve a videófolyamon keresztül elérhető eszközökkel lehet találkozni az online térben.

Barátunk, az RTSP

A modern kamerarendszerek jellemzően streaming technológiát használnak a kép- és videótartalom továbbítására. A streaming tulajdonképpen egyfajta közvetítésként értelmezhető, ahol a kliens nem tölti le a teljes videóállományt, hanem egy azonnali adatfolyamot kap és jelenít meg.

A *Real Time Sreaming Protocol* (RTSP) a streaming szolgáltatás vezérlési protokollja, amelyen keresztül a kliens kapcsolódhat az adatfolyamhoz, illetve bizonyos vezérlési funkciókkal szabályozhatja azt. Ilyen vezérlések lehetnek a *PLAY, PAUSE, RECORD* vagy egyéb szabványos parancsok. Az RTSP protokoll 1998-ban került szabványosításra[2], jelenleg a 2.0-ás verziónál tart. Az RTSP 2.0 nem teljesen kompatibilis az 1.0-ás verzióval, és bár 2016-ban jelent meg a szabvány[3], jelenleg még sokkal több eszköz használja az 1.0-ás verziót.

Alapvetően tehát az RTSP protokoll a stream vezérléséért és a kapcsolat kiépüléséért felel, a multimédia tartalom azonnali (valós idejű) átvitele már a *Real-time Transport Protocol* (RTP[4]) segítségével, jellemzően UDP kapcsolaton keresztül történik.

2004-ben jelent meg a *Secure RTP* (SRTP) protokoll[5], amely részletesen foglalkozik a biztonság kérdésével és kiegészíti az RTP-t a modern biztonsági funkciók alkalmazásával, mint például a videófolyam és más, multimédiás tartalom titkosítása vagy a visszajátszás elleni védelem.

A jelen tanulmányban megjelenő, az internetről elérhető és hozzáférhető különféle kameraeszközök beállításakor nem alkalmaztak megfelelő biztonsági szabályokat, sokszor még a legalapvetőbb hitelesítés és hozzáférés-védelem sem került beállításra, holott a legtöbb eszköz lehetővé teszi, hogy csak egy felhasználónév és jelszó birtokában lehessen a videófolyamhoz csatlakozni.

Nagyon fontos leszögezni, hogy a probléma ebben az esetben nem a gyártó hibájából fakad. Nem arról van szó, hogy a fejlesztéskor elkövetett hiba miatt, egy sérülékenységet kihasználva, vagy a protokoll gyengesége miatt férhet hozzá jogosulatlan személy a kamerához vagy a videófolyamhoz.

A hozzáférés szabályozásának hiánya a felhasználóhoz köthető, illetve ahhoz, aki a kamerát beállította és bárki számára elérhetővé tette az internet felől. A helytelen beállításnak köszönhetően bárki (aki az adott eszköz megtalálja az interneten) egy megfelelő videónéző alkalmazással (például VLC, QuickTime, stb) képes csatlakozni a kamerához, fogadni a videófolyamot vagy a képi állományokat, illetve bizonyos esetekben lehetősége lehet a kamerák vezérlésére is.

Barátunk, a HTTP(S)

Sok olyan kameramegoldás létezik, amely a webes csatornát használja a képek vagy a videófolyamok megjelenítéséhez. Ilyen esetekben a képet vagy a videót a böngészőben lehet

---

[2] *https://tools.ietf.org/html/rfc2326*

[3] *https://tools.ietf.org/html/rfc7826*

[4] *https://tools.ietf.org/html/rfc1889*

[5] *https://tools.ietf.org/html/rfc3711*

megtekinteni és felügyelni. A képek általában a szabványos HTML-en keresztül jelennek meg, azonban a videófolyam megtekintéséhez jellemzően szükséges valamilyen böngészőkiegészítő (*plugin*). Az olcsóbb, egyszerűbb kamerák esetében előfordulhat, hogy a videófolyam helyett a képek gyakori (például 10 másodpercenkénti) frissítésével érik el a „videószerű" hatást.

Sajnos sok esetben az eszközök beállításánál a felhasználók (vagy az üzembe helyezők) nem járnak el kellő gondossággal, ezáltal lehetőséget biztosítanak arra, hogy jogosulatlan személyek is hozzáférhessenek a videófolyamhoz vagy az éppen rögzített képhez.

Ehhez elegendő lehet akár az eszközzel érkezett, alapértelmezett jelszó cseréjének elfelejtése, vagy olyan jelszavak használata, amelyek könnyen kitalálhatók, például automatikus eszközök segítségével.

Még rosszabb eset lehet, ha a telepítés után egyáltalán nem kerül jelszó beállításra, így igazából a támadónak erőfeszítést sem szükséges tennie azért, hogy belepillanthasson a kameraképbe, azon keresztül pedig akár a magán- vagy a munkahelyi életbe.

A HTTP(S)-alapú webes kamerák esetében gyakran tapasztalható, hogy az adott eszköz felhasználónevet és jelszót kér a webes felületén, azonban az eszközkeresőkben (például Shodan) hitelesítés nélkül is megjelenik a kép.

Ennek oka lehet, hogy az adott eszköz olyan beállítással, esetleg authorizációs hibával rendelkezik, amely a képhez vagy a videóhoz való hozzáférést lehetővé teszi, egy adott URL meghívásával.

Ilyen hiba volt például az egyik oka a *Mirai* botnet terjedésének az *XM NetSurveillance* kamerák esetében 2016-ban, amikor ugyan a webes felület valóban kért felhasználó nevet és/vagy jelszót, azonban a *DRV.htm* meghívásával hitelesítés nélkül hozzá lehetett férni a kamera beállításaihoz[6].

Az ilyen hibák természetesen súlyos sérülékenységeknek számítanak (amelyeket a gyártók előbb-utóbb javítanak), azonban nagyon sok esetben a felhasználók nem frissítik az eszközöket, illetve nem állítják be a megfelelő védelmet rajtuk.

Természetesen tudatos megfontolás is állhat a kamera korlátozás nélküli elérésé mögött. Egy közlekedési dugót figyelő vagy éppen látképet rögzítő kamera esetén a tulajdonos, illetve az üzemeltető szándékosan teszi elérhetővé a kameraképet. Sajnos azonban nagyon sok esetben a biztonsági kamerák, vagy az otthonvédelmi kamerák esetében sem alkalmaznak megfelelő védelmet, és nem kötik jogosultsághoz az elérést.

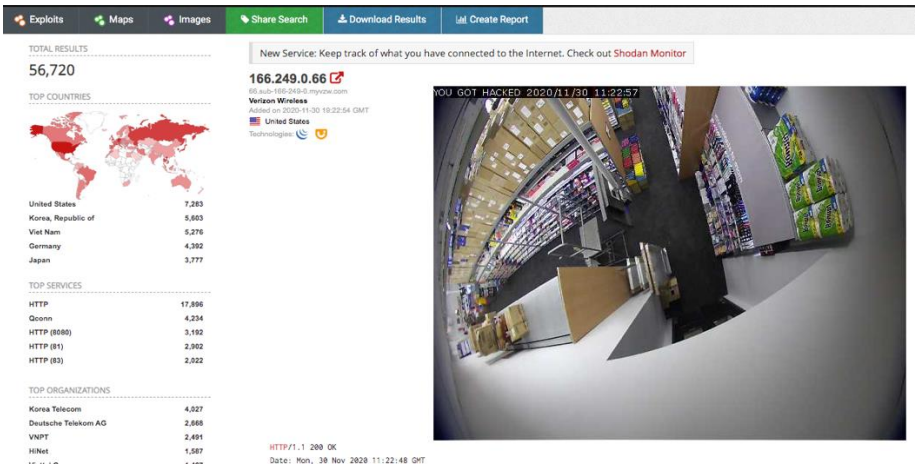
Nemzetközi és hazai körkép

Nemzetközi helyzet

Mikor a hozzáférés szabályozás nélküli, webes felületen keresztül elérhető kamerákat kerestük, a Shodan eszközkereső legalább 56 720 olyan kamerát tartott nyilván, amelyek esetében a kereső

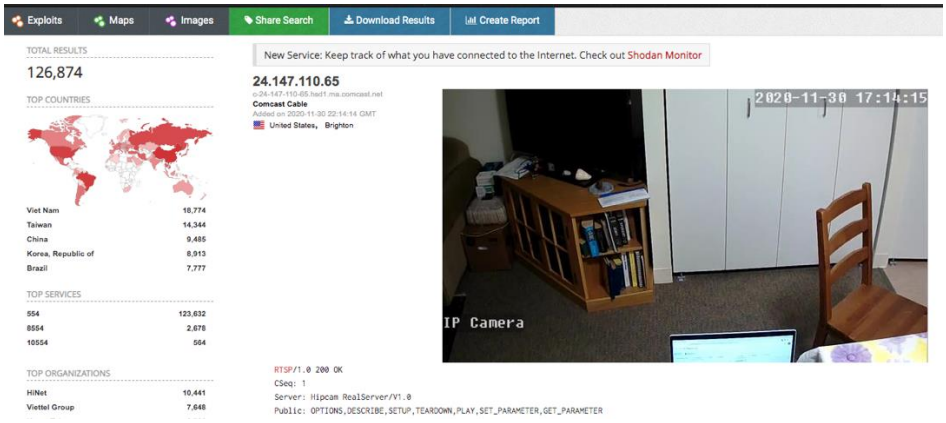
[6] *https://threatpost.com/when-dvrs-attack-a-post-iot-attack-analysis/121179/*

képes volt a képekhez hozzáférni. Ez természetesen azt is jelenti, hogy bárki más is láthatja a kameraképeket.



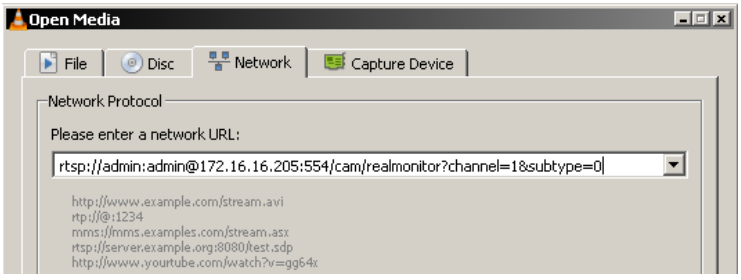
Shodan eszközkereső, több mint 50 ezer hozzáférhető webes kamera világszerte

Az streaming-képes, RTSP-alapú kamerák közül 4.4 millió eszköz érhető el az interneten, azonban „csak" 126 874 olyan, amelyhez felhasználónév és jelszó nélkül is csatlakozni lehet, és amelyek esetében a videófolyam hozzáférhető.



126 874 hitelesítést nem elváró streaming-képes kamera eszköz az interneten

A csatlakozáshoz nincs szükség speciális szoftverre, elegendő hozzá a sokak által ismert és használt VLC (vagy QuickTime) videónéző, amely képes RTSP kapcsolatot kiépíteni a kamerákkal (vagy a videófolyamot továbbító és rögzítő DVR berendezéssel).



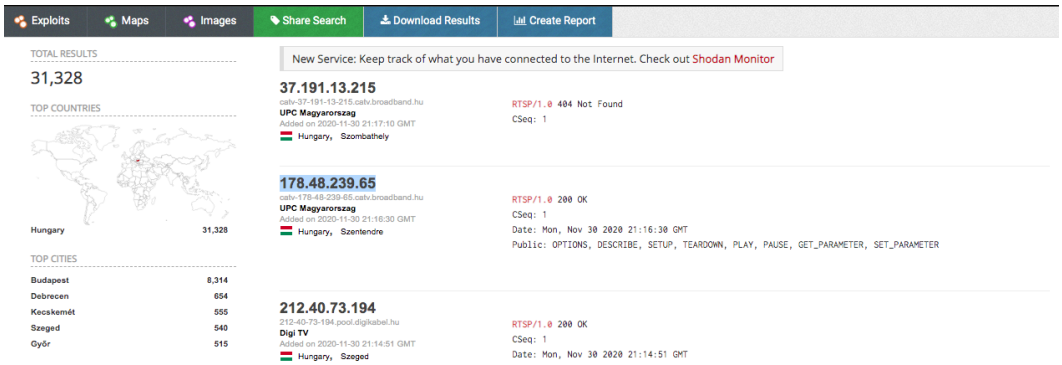
VLC beállítás péda (itt felhasználónév és jelszó megadásával)

A VLC beállításban is látható, hogy van lehetőség a videófolyamhoz való hozzáférést felhasználónévhez és jelszóhoz kötni, azonban a csaknem 127 000 eszközön nem éltek ezzel a biztonsági beállítással, ezáltal bárki képes kapcsolódni a videófolyamokhoz.

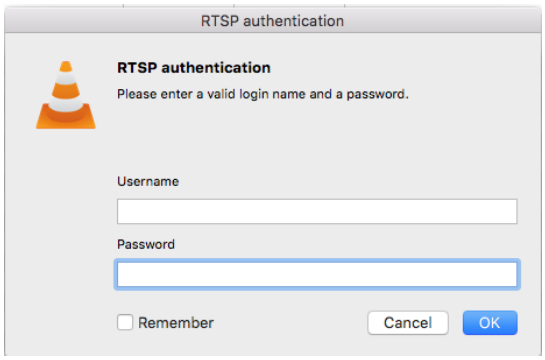
A hazai helyzet

Streaming-képes eszközök (RTSP)

A streaming-képes kamerák esetében a Shodan eszközkeresővel jelen tanulmány megírásakor több mint 31 328 hazai eszköz volt fellelhető. Ezek a kamerák lehetővé teszik az RTSP-alapú kapcsolatot és a videófolyam elérését, azonban a kamerák többsége helyesen van beállítva és elvár valamilyen hitelesítést a kapcsolódáskor.



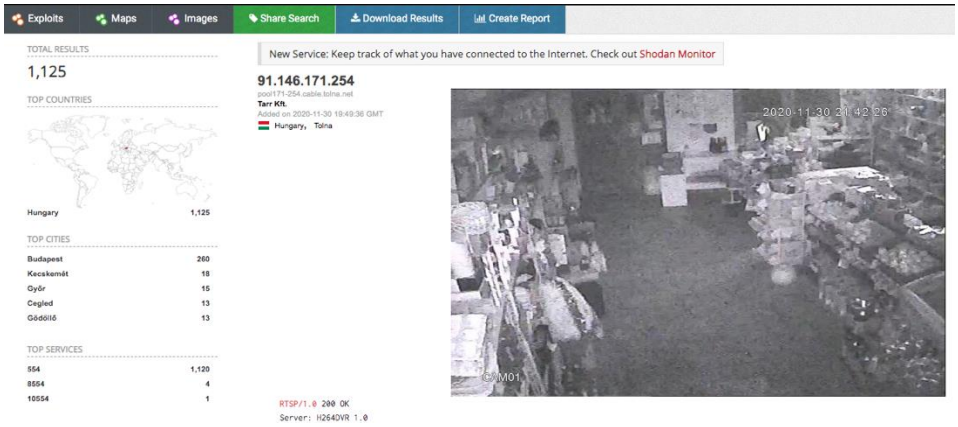
31 328 streaming-képes hazai eszköz a Shodan eszközkeresőben



A VLC felhasználót és jelszót kér csatlakozáskor

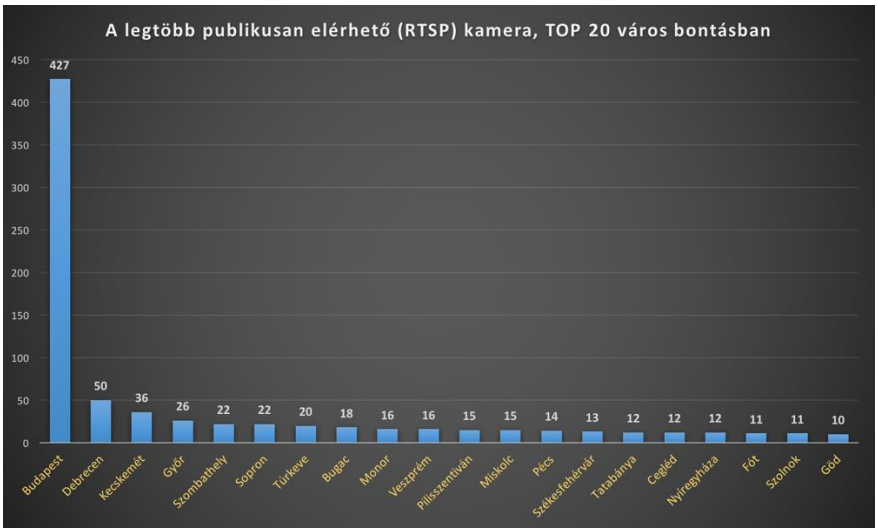
A Shodan eszközkereső az interneten megtalált kamerákhoz megpróbál csatlakozni, és ha az eszköz nem vár el hitelesítést, a kereső képes képernyőképet készíteni a videófolyamról. A képernyőmentés elérhető a keresőben, így arra is van lehetőség, hogy szűrőfeltételt megadva csak olyan eszközöket jelenítsen meg, amelyekről rendelkezésre áll képernyőmentés (*screenshot*).

A Shodan kereső jelen tanulmány megírásakor legalább 1125 olyan hazai, streaming-képes kamera eszközt tartott nyilván, amelyen nem állítottak be hozzáférés védelmet és a készülék nem kér felhasználó nevet és jelszót a videófolyam megtekintéséhez.



1125 hazai, szabadon elérhető, streaming-képes kamera, képernyőfotókkal[7]

A Shodan által készített képernyőfotókat ellenőrizve megállapítható, hogy meglehetősen széles a streaming-képes kamerák felhasználási területe. Megtalálhatók köztük a különféle objektumvédelmi célokra alkalmazott biztonsági kamerák, a kültéri megfigyelő eszközök, bevásárlóközpontok és boltok beltéri kamerái, babafigyelő eszközök, otthoni beltéri és kültéri kamerák, stb. Bár a 31 ezer hazai eszköznek csak 3.5%-a érhető el minden korlátozás nélkül, nemzetközi viszonylatban ez az arány kicsit alacsonyabb, 2.8%.



A feltehetőleg rosszul beállított kamerák többsége Budapesten található.

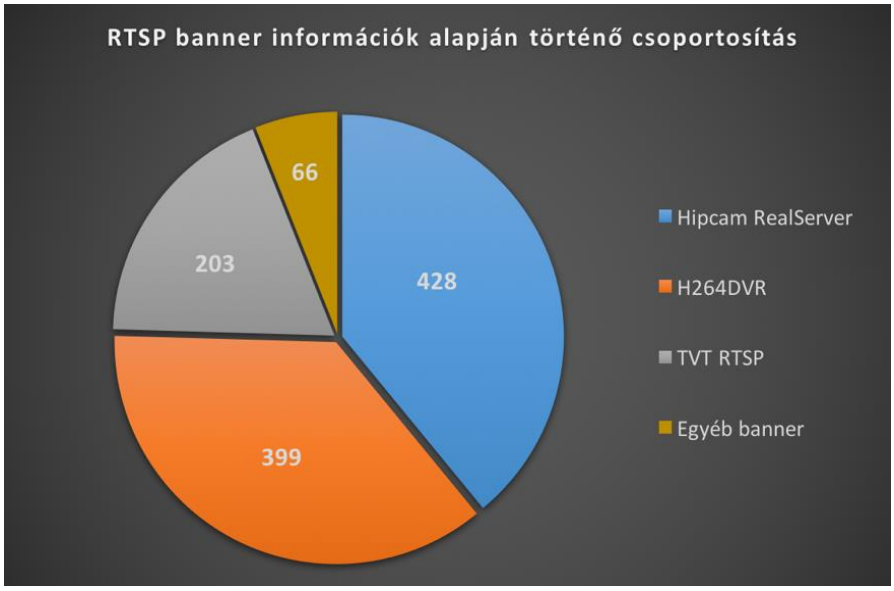
Az eszköztípusok azonosítása meglehetősen nehézkes. Ahogy a korábbiakban említésre került, az OEM gyártók eszközei akár száz különböző „gyártó" neve alatt is forgalomba kerülhetnek, A Xiongmai (*Netsurveillance*) kamerái például ASECAM, AZISHN, BESDER/BESDERSEC, ESCAM, FLOUREON, GADINAN, HAMROL, HAMROLTE, Hiseeu, KKMOON, MISECU, Techage, Techege, Unitoptek, USAFEQLO eszköznevek alatt is megjelenhetnek[8].

A Shodan kereső adataiból legyűjtve három nagyobb hazai eszközcsoport azonosítható, azonban a banner információk alapján is legfeljebb a beágyazott alkalmazástípust lehet meghatározni.

---

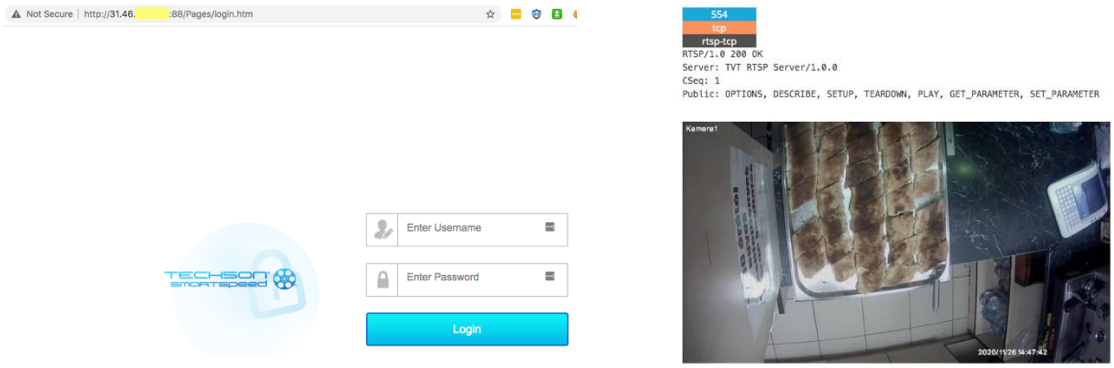
[7] Az adatgyűjtés és a kép két külön időpontban készült, három nap eltéréssel. Az adatgyűjtéskor 1095 eszköz volt elérhető, míg a kép készítésekor már 1125. A statisztika az 1095 eszközt tartalmazó lista alapján készült.

[8] https://bitekmindenhol.blog.hu/2020/08/21/ip_kamera_lan_besder_960p



A három alkalmazástípus banner információ-alapú azonosítása

A *Hipcam Real Server* a Hipcam fejlesztése, amelyet sok egyéb gyártó is OEM licenszel. Nemzetközi szinten legalább 115 000 olyan eszköz érhető el az interneten, amelyben a Hipcam alkalmazása fut. A H264DVR banner információval rendelkező készülékek jellemzően XiongMai (*Netsurveillance*) eszközök, illetve azok valamely OEM-licenszelt változata. A TVT RTSP banner információ pedig jellemzően a *Techson Smartspeed*, illetve kisebb számban *Provision Isr* eszközöket jelenti. Az egyéb kategóriában továbbá megtalálhatók például a *Vacron* vagy a *Hikvision* eszközei is.

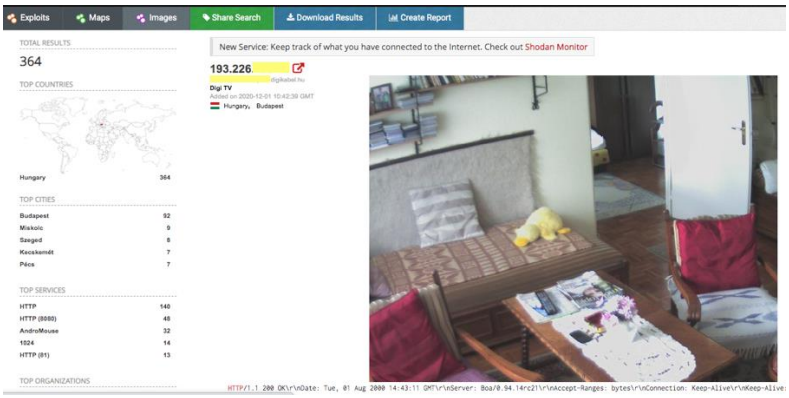


Techson Smartspeed web és RTSP – avagy rétesezett biztonság

Provision Isr web és RTSP – avagy a csipkés értékvédelem

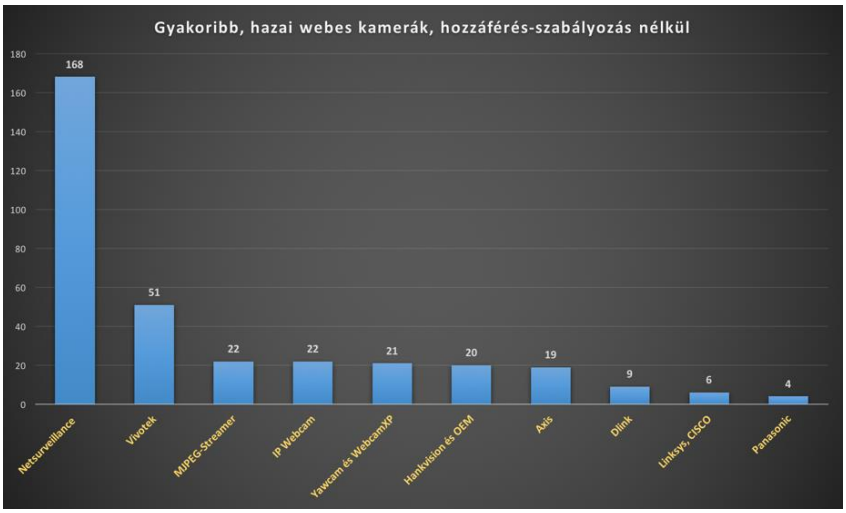
Webes kamerák

A különféle webes felületeken elérhető kamerák esetében megállapítható, hogy jóval kevesebb olyan eszköz kapcsolódik az internetre, amely a webes felületén keresztül jeleníti meg a médiatartalmat, és amelyek nem rendelkeznek megfelelő hozzáférés-védelemmel.



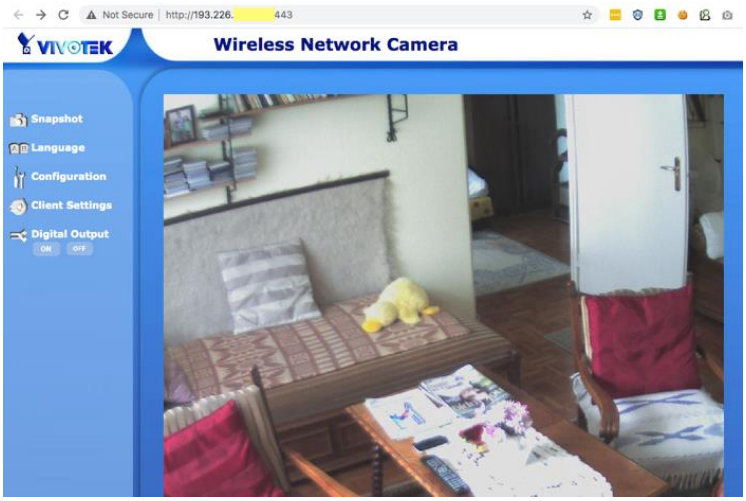
Hazai, webes felületről elérhető kamerák, amelyek lehetővé teszik a képhez történő hozzáférést

Legalább 364 olyan eszköz található a hazai interneten, amelyek esetében a kamerakép bárki számára hozzáférhető. Az eszközök között megtalálhatók olyan kamerák, amelyek tájékoztatási feladatot látnak el, mint például látkép, dugó- vagy gólyafigyelő kamera, azonban az eszközök jelentős része valamilyen otthoni, munkahelyi, objektumvédelmi megfigyelő, vagy biztonsági eszköz.



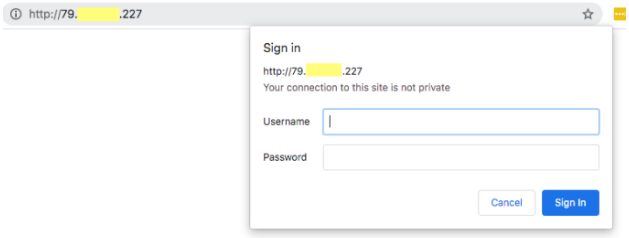
Gyakoribb, hazai web elérésű kamerák, hozzáférés-szabályozás nélkül

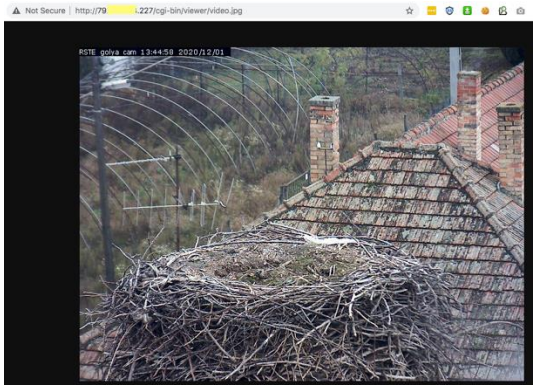
A kamerák vizsgálatakor látható volt, hogy sok esetben a jelszavas védelem beállítása sem történt meg, a kamerakép, illetve rosszabb esetben akár a beállítási felület is szabadon hozzáférhető.



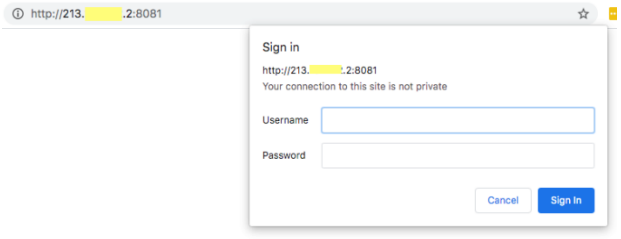
Vivotek otthoni kamera, bárki csatlakozhat és akár konfigurálhatja is

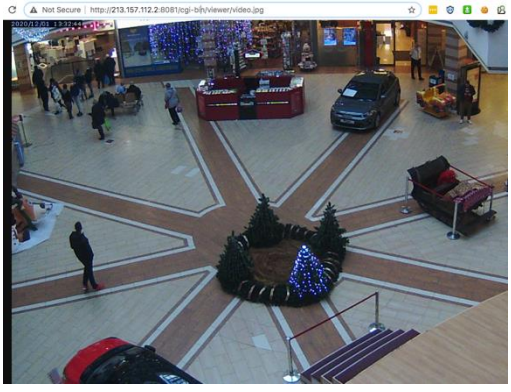
A Shodan eszközkereső képes az ismertebb kameratípusok azonosítására, azaz, ha az eszközkereső robotja megtalál és kameraként ismer fel egy eszközt, megpróbálja az eszköztípust is meghatározni. Ezzel együtt az ismertebb kamerák különféle statikus *snapshot,* valamint akár az elérhető videófolyam címeit is meghívja. Ha a hozzáférés korlátozás nincs kiterjesztve a statikus képre (vagy videófolyamra), akkor a Shodan lementi az aktuális képet a kamerából.





A kamera a webes felületen jelszót kér, de a "*cgi-bin/viewer/video.jpg*" bárki számára elérhető



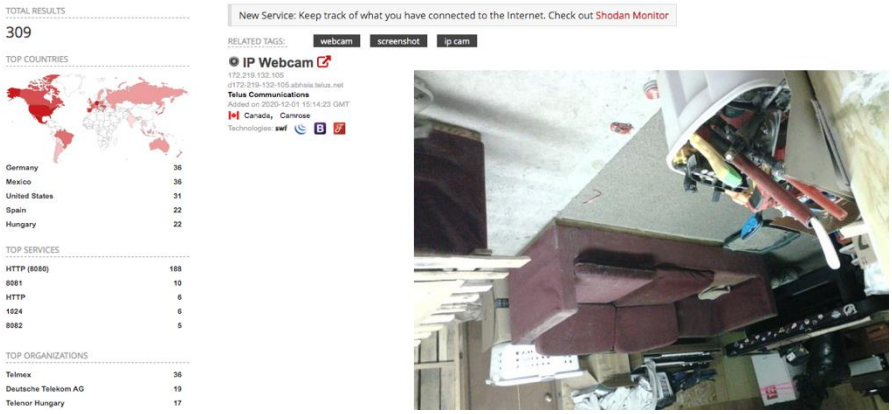


Ugyanez a beállítási hiba egy pláza esetén sokkal problémásabb, mint egy gólyafigyelő esetében

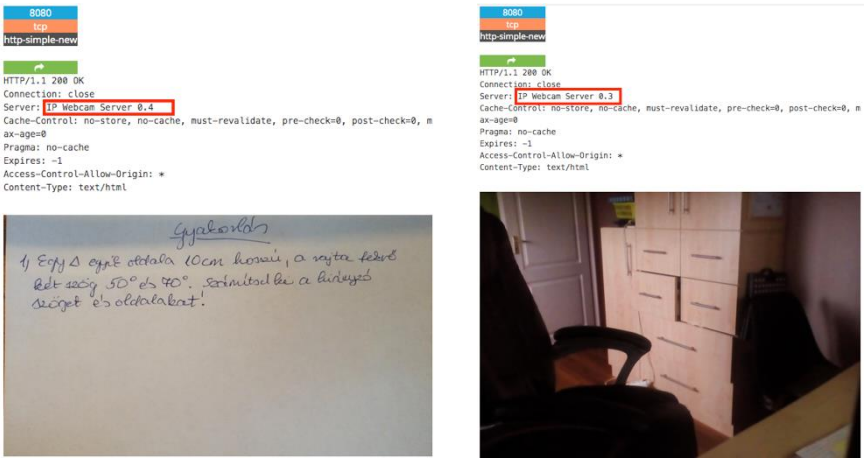
Kamera RTSP paramétereinek kiolvasása

A hazai, hozzáférhető webes felületen elérhető kamerák típusaival kapcsolatban megállapítható, hogy jellemzően *Netsurveillance* (151 darab), *Vivotek* (51 darab), *Hankvision* vagy OEM klón (20 darab) eszközök. Kisebb számban megtalálhatók az *Axis*, *Trendnet*, *Dlink*, *Sercom* OEM klón, *Yawcam*, *WebcamXP*, *Lynksys*, illetve *CISCO* készülékei is.

Érdemes megemlíteni az *IP Webcam*[9] megoldásokat, amelyekből nemzetközi szinten 309, a hazai szinten pedig 22 darab hozzáférhető eszköz volt fellelhető az online térben. Az *IP Webcam* egy Android alkalmazás, amely a mobiltelefonból „csinál" mozgásérzékelő webkamerát. Sajnos a tapasztaltak szerint ezekben az alkalmazásokban sem állították be a felhasználónév és jelszó elvárását a csatlakozáshoz.



309 nemzetközi IP Webcam, amelyek rögzített képe hozzáférhető



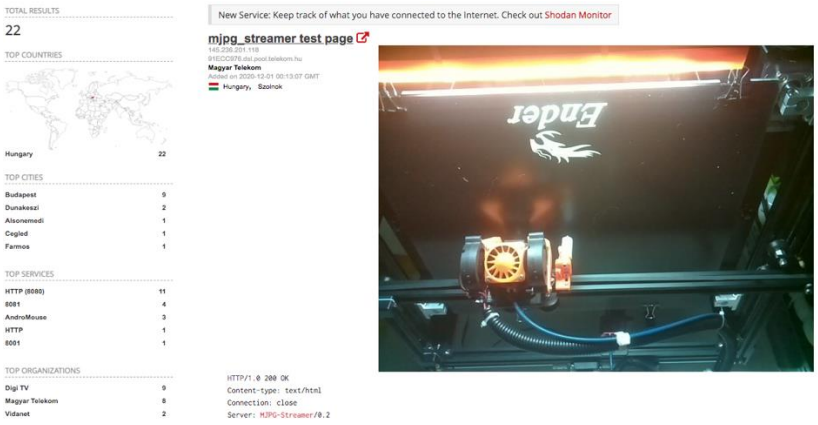
Hazai IP Webcam megoldások – hitelesítési elvárás nélkül

[9] *https://play.google.com/store/apps/details?id=com.pas.webcam&hl=en_US&gl=US*

Ugyancsak érdekes megoldásnak számítanak az *MJPEG-Streamer* alapú eszközök, amelyeket a „*szegény ember streamingjének*” is szoktak nevezni.

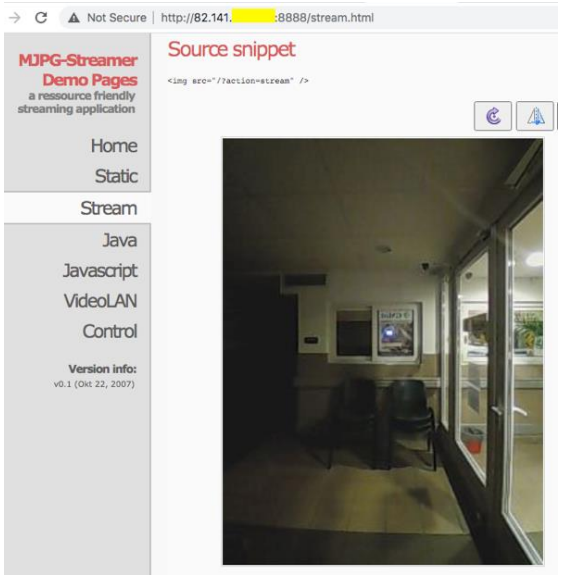
Az *MJPEG-Streamer* program a csatlakoztatott webkamerából olvassa ki a képi állományt, majd HTTP csatornán továbbítja a megtekintő vagy kliens felé. Mivel a kép tömörítése a kamerában történik, az olvasó eszköznek nincs szüksége sok erőforrásra a kép kiolvasásához és közvetítéséhez, így előszeretettel használják a programot a különféle beágyazott rendszerekben, például Raspberry Pi, vagy más, egylapkás eszközökben (akár OpenWRT-alapú routerekkel kombinálva).

Nemzetközi vonatkozásban 973 *MJPEG-Streamer* alapú megoldás érhető képi hozzáféréssel az internet felől, amelyekből 22 a hazai eszköz. Bár az ilyen eszközökben is megvalósítható legalább a felhasználónév és jelszó kérése, ezek a berendezések sem várnak el hitelesítést, így a kameraképek bárki számára hozzáférhetők.



22 hazai MJPEG-Streamer eszköz, felhasználónév és jelszó kérés nélkül

A Shodan által rögzített, illetve a nyilvánosan elérhető képeket megvizsgálva szerencsére ez talán nem jelent magas kockázatot, mivel a hazai eszközök többségükben valamilyen berendezés (például 3D nyomtató) megfigyelésére használt *Do-It-Yourself*, azaz házilag épített megoldásoknak tűnnek, amelyeket feltételezhetően szándékosan tettek ilyen módon elérhetővé.

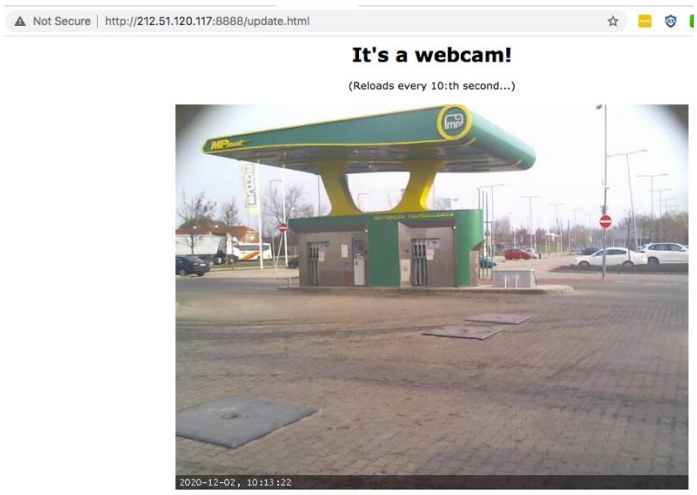


Hazai példa, amikor nem egy berendezés megfigyelésére használják a megoldást

Nem csak a fixen telepített webes elérésű kamerák beállításakor járhatnak el a felhasználók és tulajdonosok óvatlanul.

A vizsgálatkor több olyan kameramegoldás is fellelhető volt, amelyek a klasszikus webkamerák családjába tartozhatnak, azaz olyan eszközök, amelyeket egy laptophoz vagy asztali számítógéphez csatlakoztattak és egy webkamera szoftver segítségével jelenítették meg a videótartalmat. Ilyen megoldások lehetnek a *Yawcam* és *WebcamXP* videókamera szoftverek, amelyekből hazai vonatkozásban 21 darabot sikerült azonosítani.

Példa a Yawcam kameraszoftver személyes felhasználására



Példa a Yawcam kameraszoftver megfigyelő célú felhasználására

Ezeket a megoldásokat jellemzően szintén megfigyelő kamerának szánják, azonban ebben az esetben is tapasztalható a személyes célú felhasználás.

Kockázatok és mellékhatások

A következőkben olyan problémák és kockázatok kerülnek felsorolásra, amelyek a biztonságtudatosság hiányából, az internetről elérhetővé tett kamerák esetleges sérülékenységéből vagy az eszközök helytelen beállításaiból adódhatnak.

A felhasznált képeket a Shodan eszközkereső olvasta ki a megtalált kamerákból. A képek jelen tanulmányban való felhasználásának célja, hogy felhívja a figyelmet a helytelen kamerahasználatból fakadó lehetséges veszélyekre.

Magánélet, intimszféra sérülése

Talán a magánéletet és privát szférát érintő kockázatok azok, amelyek bárki számára egyértelműek lehetnek. A hibás beállításokból, vagy a felhasználó biztonságtudatosságának hiányából, illetve az eszközök sérülékenységéből adódóan a nyilvánosság számára elérhetővé tett otthoni kamerák, a rögzített vagy megjelenő képek és videófolyamok idegenek számára teszik lehetővé, hogy belepillantsanak magánéletükbe és megsértsék a magán-, rosszabb esetben akár az intim szférát.

A magánélethez való jog az emberi méltóságból levezetett és a Polgári Törvénykönyvben külön nevesített személyiségi jog. Az Alaptörvény VI. cikkének (1) bekezdése leszögezi, hogy „*Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák*".

A magánélet védelme több, egymástól eltérő terület együttes védelmével valósulhat meg. Ide tartozik a személyes adatok védelme, a családi élet és magánlakás, valamint a magántitok, levéltitok védelme is. E védelmek eredménye a magánélet zavartalansága[10]. A magánélethez való jog védelmének egyik alappilére a 2018. évi LIII. törvény a magánélet védelméről, amelynek 2. § (3) pontja kimondja, hogy: *„A magánélethez való jog lényege, hogy azt - külön törvényben meghatározott kivételekkel - az egyén akarata ellenére mások ne sérthessék meg.*"

A törvény ebből a szempontból egyértelműsíti a 7. § (1) pontban, hogy „*Mindenkinek joga van arra, hogy magánéletét fokozott védelem illesse meg, és azt más előtt csak saját akaratából vagy törvényben meghatározott esetben fedje fel.*"

Biztosan állítható, hogy az otthon üzemelő, rosszul beállított és helytelenül működtetett kamerák nem a tulajdonos akaratával egyezően teszik elérhetővé bárki számára a kameraképeket és videófolyamokat. Bár a kamerák internet felőli elérését feltehetőleg a tulajdonos tette szándékosan vagy véletlenül lehetővé, azonban az akaratában az biztosan nem szerepelt, hogy a kamerán keresztül idegen személyek lássanak bele a magánéletébe.

A törvény szerint az állam jogi védelemben részesíti az otthon nyugalmát. A 10. § (1) pont kimondja, hogy „*Az otthon nyugalma biztosítja a magán- és családi élet kibontakozását, továbbá a magánszféra szabad és teljes megélését. Ennek tiszteletben tartása érdekében mindenkinek az otthonát mint magánéletének, családi életének színterét fokozott védelem illeti meg.*"

Látható tehát, hogy ebben az esetben a szándékosan vagy a biztonságtudatosság hiányából fakadóan korlátozás nélkül elérhetővé tett kameraeszközök a tulajdonos és a felhasználó (vagy akár a család) magánélethez való jogát sértik – azonban, ha a beállításokat maga a tulajdonos végezte, a felelősség és az elszenvedett kár egyértelműen a tulajdonost (és egyben magát a lehetséges sértettet) terheli.

Eltérő a helyzet akkor, ha az eszközöket más, például egy szolgáltató, vagy biztonságtechnikai cég létesítette és állította be hibásan, vagy ha a kamerák esetleges biztonsági hibája miatt sérül a tulajdonos és működtető magánélethez való joga. Az első esetben természetesen az eszköz telepítője, míg a második esetben az eszköz gyártója lehet a felelős, azonban az utóbbi esetben is

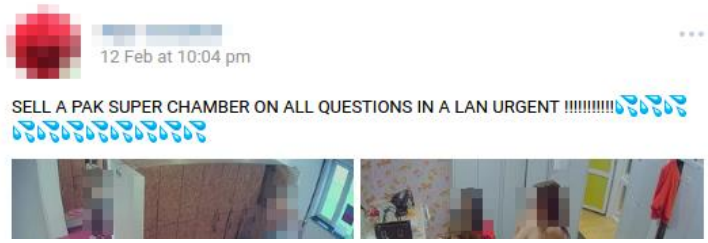
[10] *https://u-szeged.hu/efop362-00007/minden-szocikk/maganelet-zavartalansaga*

felmerül a kérdés, hogy a tulajdonos járhatott volna-e el gondosabban, és vajon megtett-e mindent azért, hogy magánéletéhez való joga ne sérüljön?

Általános álláspont, hogy bármely informatikai berendezés tartalmazhat olyan hibákat, amelyek kockázatot jelenthetnek a felhasználója számára. Az otthoni kameraeszközök felhasználójának felelőssége kiterjed az eszközök biztonságos működtetésére is. Ebbe nemcsak az tartozik bele, hogy az eszközt rendeltetésszerűen használja, hanem az is, hogy az eszköz kiberbiztonságával kapcsolatos teendők is rá hárulnak, például a megfelelő frissítések és biztonsági javítások telepítése is a felhasználó feladata.

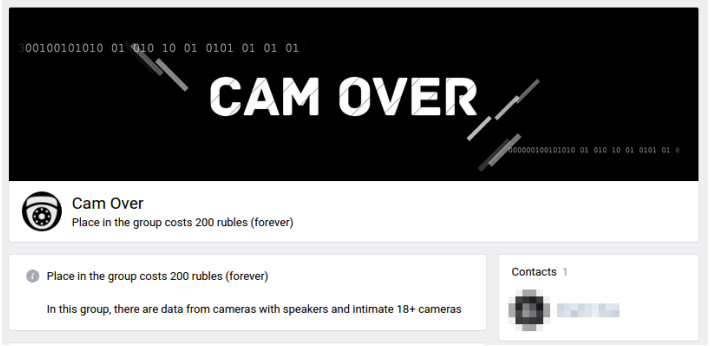
Nagyon sok hír szól arról, hogy a különféle hostelek, apartmanházak vagy Airbnb szállások vendégei rejtett kamerákat találtak, amelyeken keresztül idegenek leshették meg őket. (Meglehetősen sok ilyen rejtett kamerás tartalom érhető el a felnőtt oldalakon.) Ugyanez a lehetséges kockázat akkor is, ha a felhasználó otthonában hibásan beállított, vagy sérülékeny és elérhetővé tett kamerák üzemelnek: a tulajdonos és családja ki vannak téve a leskelődés, zaklatás és a megszerzett adatokkal történő különféle visszaélésekkel szemben (például zsarolás, lejáratás, nyilvánosságra hozás, videóoldalakra feltöltés, vagyonelleni bűncselekmények, stb.).

2020 októberében jelent meg egy hír egy hacker csoport működéséről, amely 50 000, többségében szingapúri és otthoni kamerát hackelt meg, majd adta el a felvételeket[11]. A kb. 3TB mennyiségű videóért 200 dollár körüli összeget kértek. A csoport a lopott videókból jellemzően intim jeleneteket tartalmazó videókat töltött fel különféle felnőtt oldalakra.



Lopott kamerafelvételek értékesítése *(forrás:TrendMicro)*

A különféle feketepiaci vagy DarkNet csoportok és fórumok oldalain is kínálják, illetve vásárolják akár a kamerákhoz való hozzáférések eszközeit (streaming adatok, szoftverek, jelszavak, sérülékenységek, stb), vagy akár a már megszerzett képeket és felvételeket.



Kamerás csoport, 200 rubel életre szóló tagságival *(forrás: TrendMicro)*

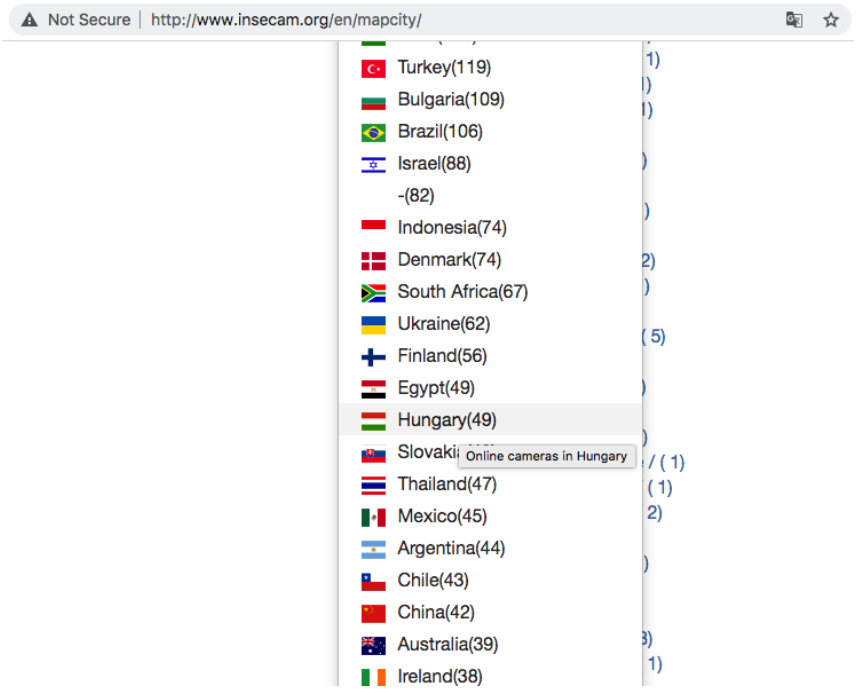
[11] *https://www.tnp.sg/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams*

Jelen tanulmány elkészítéséhez a Shodan eszközkereső nyújtott segítséget, azonban minden szakismeret nélkül is lehet rosszul beállított kamerákból képeket vagy videófolyamot szerezni. Több olyan oldal is elérhető, amely a hozzáférhető kamerákból jelenít meg tartalmat, vagy az ilyen kamerákat összegyűjtve kínálja a listát a leskelődőknek.

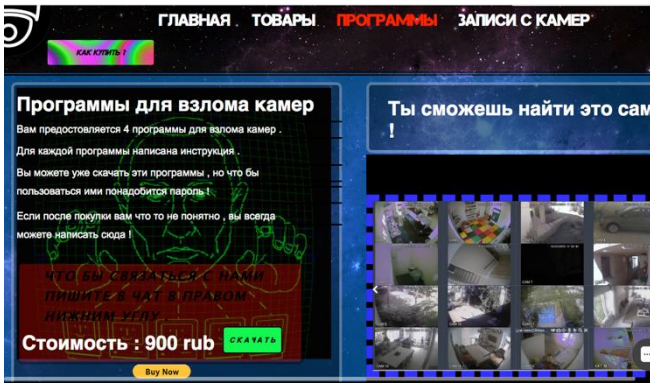
Olyan oldalak is léteznek, amelyek szervezetten értékesítik a kompromittált kamerákból származó, jellemzően intim jeleneteket is tartalmazó felvételeket. Még hazai weboldal is található, amely üzletet csinál a felvételek megszerzéséből és kiszivárogtatásából. Külön érdekesség, hogy bár a cím .hu domain végződésű, az oldal tartalma orosz nyelvű.

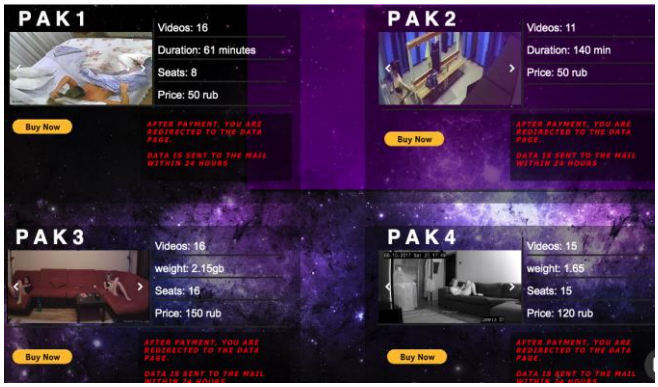
Az olyan oldalak, mint az *insecam.org* vagy az *ip-scan.ru* elvégzi a keresést a leskelődő helyett, neki pedig már csak választania kell, mely ország, mely város kameráira kíváncsi.

Szerencsére Magyarország erősen alul reprezentált ezeken az oldalakon, azonban a magánélet megsértésének fenyegetése folyamatosan növekszik: a hasonló oldalak segítségével, képzettség és szakismeret nélkül is válhat bárkiből leskelődő.



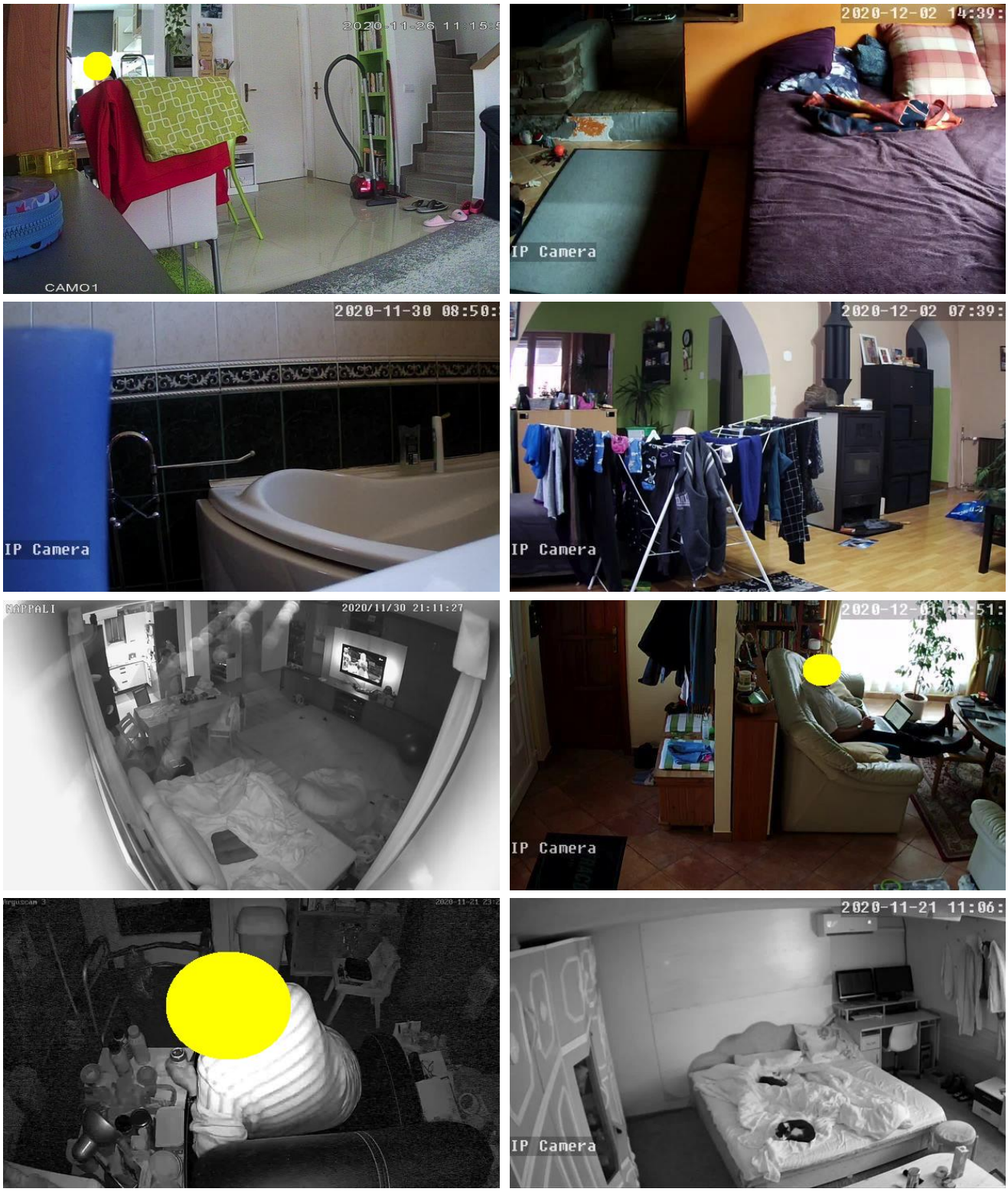
Szerencsére hazánkból csak 49 kamerát jelenít meg az oldal





Hazai domainen hosztolt orosz nyelvű oldal, kiszivárgott videók és hacker eszközök értékesítése

Néhány példa az elérhetővé tett, otthoni biztonsági kamerák világából[12]



[12] *Az előzőekben, illetve a későbbiekben is szerepelnek olyan képek, amelyek az otthon és a magánélet sérülésének kockázatát mutatják be.*


2020-11-28 04:30:
IP Camera


2020-11-21 03:32:
IP Camera


2020-11-23 19:15:
Mani kamera

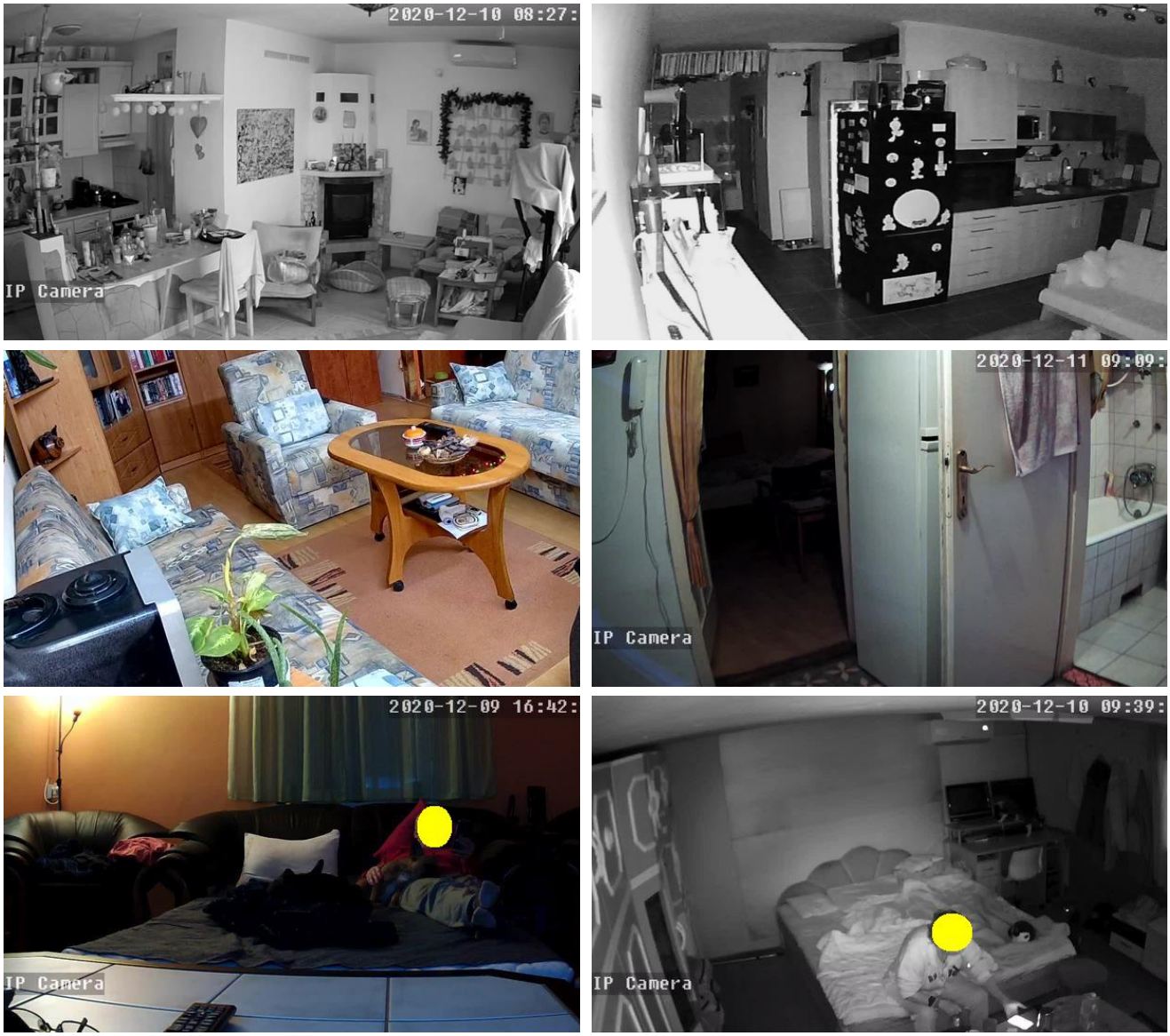

Csepel nappali


2020-12-02 21:13:
IP Camera


2020-12-03 02:44:
IP Camera


2020-12-03 10:06:


2020-12-03 17:33:
IP Camera



Sérülékenységek, sebezhetőségek

Sajnos még abban az esetben is jelenthetnek kockázatot a különféle kamerák, ha a felhasználó megfelelő gondossággal járt el a beállításukkor. Ha a kamera vagy megfigyelőrendszer elérhető az internet felől, számolni kell azzal a lehetőséggel, hogy egy esetleges sérülékenység miatt jogosulatlan személyek férhetnek hozzá a kameraképhez vagy videófolyamhoz.

Meglehetősen sok cikk és kutatás lelhető fel[13], amely a különféle olcsóbb, nagyrészt kínai kamerák veszélyeire hívják fel a figyelmet, de a szakértők vizsgálódásai nem korlátozódnak csak a kínai OEM megoldásokra. Sérülékenységeket találtak többféle kameraeszközben is,

---

[13] Balázs Zoltán, az egyik legkiválóbb hazai biztonsági szakember kalandja a saját, otthoni célra vásárolt eszközével mindenképpen fontos kiindulópont annak, aki a kamerák biztonságával kapcsolatban végez kutatásokat.

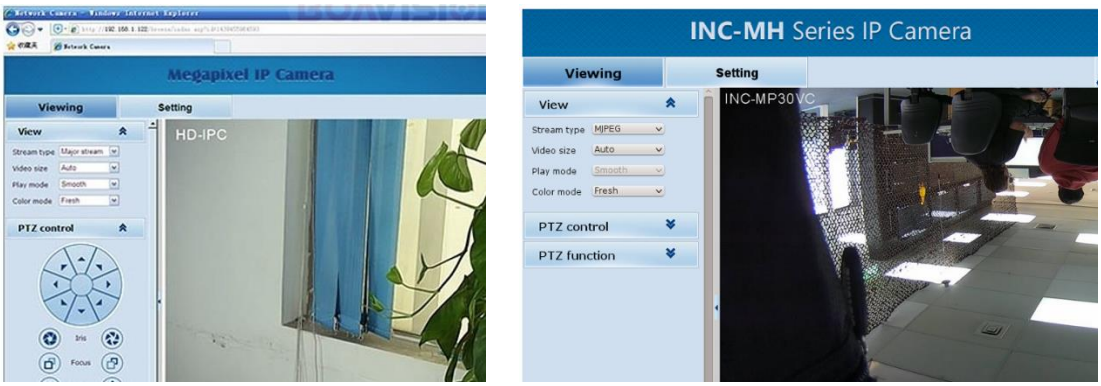
például a Google Nest, Ring, D-link, Axis, Avtech (és lehetne még tovább sorolni) bizonyos kameráiban is.

Még 2012-ben a Trendnet bizonyos eszközeivel kapcsolatos sérülékenység után bukkantak fel különféle, sérülékeny Trendnet eszközöket tartalmazó listák az interneten. A listák segítségével gyakorlatilag bárki képes volt a kamerákhoz csatlakozni, és a tulajdonosok vagy működtetők után kémkedni.

690 sérülékeny Trendnet kamera, és a Google Map-integrált alkalmazás a leskelődésre

A kínai *Hankvision* a többkamerás DVR/NVR rendszerektől a forgatható PTZ kamerákig bezárólag gyárt készülékeket. Kiderült, hogy hátsóajtó (*backdoor*) található eszközeikben, amelyen keresztül be lehet jelentkezni a kamerákba[14]. Sajnos sok más „gyártó" is OEM licenszeli a megoldásaikat, így akár több tucatnyi formában és brand alatt lehet találkozni ezekkel az kamerákkal.

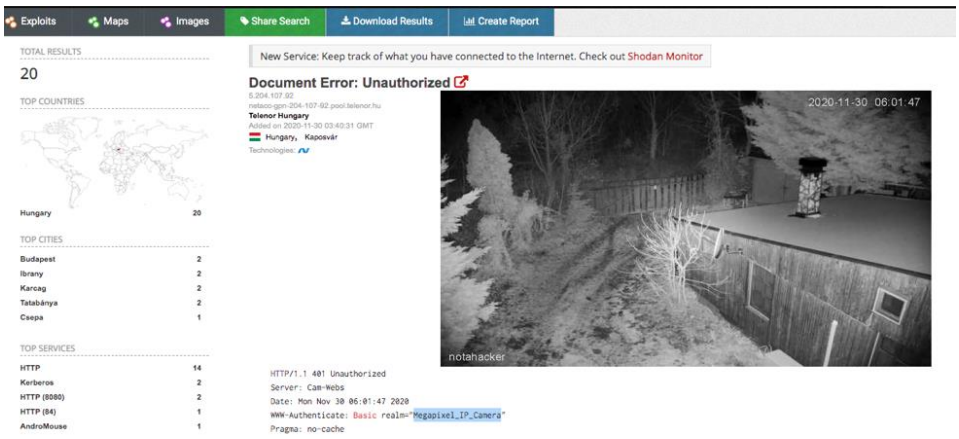
Hankvision, JideTech, Boavision – OEM licenszelt megoldások, lehetséges backdooral



Felismerhető a backdoor-gyanús eszközök webes felülete

[14] *http://sergei.nz/ildvr-inc-mh40d06-security-nightmare/*

Amennyiben a kamera webes felületének fejlécében szerepel a „Megapixel IP *Camera*" vagy az „*INC-MH Series IP Camera*", illetve a kamera webes felülete hasonlít az fentebbi felületekhez, előfordulhat, hogy a „*HANKVISION/HANKVISION*" vagy a „*HANKVISION_2016/HANKVISION_2016*" felhasználónévvel és jelszóval hozzá lehet férni az eszközhöz.



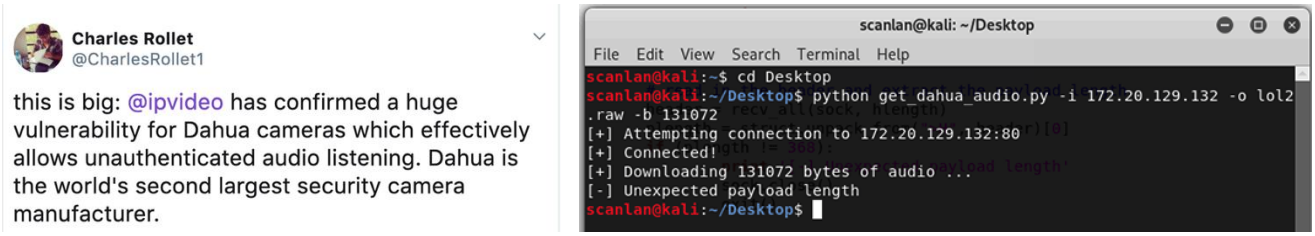
20 olyan hazai eszköz, amely esetében feltételezhető, hogy backdoort tartalmazhat

A *Hankvision* által gyártott (vagy más gyártók részére OEM licenszelt) kamerák webes felületének HTTP kommunikációs fejlécében szerepel a „*Basic realm= Megapixel_IP_Camera*" azonosító. A Shodan eszközkereső legalább 20 olyan hazai eszközt talált, amely ettől a gyártótól, vagy OEM partnerétől származik, és az eszközkereső képet tudott kimenteni belőle. Ez szerencsére meglehetősen alacsony szám, azonban nemzetközi szinten legalább 2339 ilyen eszköz található.

Az ugyancsak kínai, és a *Hikvision* után a második legnagyobb biztonsági kameragyártó *Dahua* eszközeivel kapcsolatban 2017-ben a Nemzeti Kibervédelmi Intézet is figyelmeztetést[15] adott ki, amely szerint „*Feltehetőleg a Dahua minden termékét érintő backdoor sérülékenység vált ismertté. A támadó a felhasználói adatbázist távolról letöltve bármilyen, akár rendszergazdai fiókokhoz is hozzáférhet*". A sérülékenység két problémából fakadt. Az első hibán keresztül a támadónak lehetősége volt az eszköz felhasználói adatbázisát, a felhasználónevekkel és kódolt (*hashelt*) jelszavakkal letölteni az eszközből. A második hiba miatt a kódolt jelszavakat sem kellett visszafejtenie, ha a kódolt jelszót másolta be a login felületbe, az eszköz engedélyezte a bejelentkezést (*pass-the-hash*). 2019-ben olyan, a Dahua (és Amcrest) eszközöket érintő sérülékenység látott napvilágot[16], amely lehetővé tette, hogy a támadó távolról csatlakozzon a kamerához, majd bekapcsolja a mikrofont, rögzítse és lehallgassa a helyiségben elhangzottakat.

[15] *https://nki.gov.hu/figyelmeztetesek/serulekenysegek/dahua-backdoor-serulekenyseg/*

[16] *https://ipvm.com/reports/dahua-audio?code=allow*



Lehallgatás Dahua eszközön keresztül

A képen látható, hogy a támadó bármiféle felhasználónév és jelszó megadása nélkül kapcsolódni tudott az eszközhöz, majd 131072 bájtnyi audio adatot kért és töltött le az eszközből. A leírások szerint még az sem jelentett megoldást, ha a kamera audio funkciója le volt tiltva.

Látható, hogy ha valaki ilyen kamerákat tesz elérhetővé az internet felől, még akkor is kiteszi magát egy esetleges sérülékenységet kihasználó támadónak, ha egyébként véleménye szerint mindent megtett azért, hogy a kamerát „biztonságosan" állítsa be. A biztonságos beállítás nem csak az erős jelszavakat, az alapértelmezett felhasználói nevek és jelszavak letiltását vagy cseréjét, esetleg az adatvédelmi elvárásoknak megfelelő látószöget jelentik. Ha egy eszközt elérhetővé teszünk az interneten, a magánéletet, más személyeket vagy az értékeket is kitesszük a sérülékenységekből és sebezhetőségekből fakadó kockázatoknak.

Ha az itthoni eszközöket tekintjük, a vizsgálat idején legalább 554 Dahua-alapú hazai eszköz volt elérhető az interneten. Az 554 Dahua eszköz felhasználónevet és jelszót kér a videófolyam betekintéséhez, így (csak) ebből a szempontból helyesen vannak beállítva, és a tanulmány statisztikai adatai között nem szerepelnek[17]. Azonban ismét fontos felhívni a figyelmet arra, hogy egy eszköz még akkor is veszélyessé válhat, ha hitelesítést kér a betekintéshez. Az, hogy elérhető az internet felől már lehetőséget biztosíthat a támadónak, hogy megpróbálja kihasználni az eszköz esetleges sérülékenységét, és megkerülje a megtett védelmi intézkedéseket.

Az Egyesült Államok kormánya a *Huawei* mellett egyébként a *Hikvision* és *Dahua* termékeket, megoldásokat és alkatrészeket is tiltólistára tette, és kormányzati intézményekben vagy kormányzathoz tartozó szervezeteknél történő alkalmazásukat 2019 augusztusában betiltotta.[18]

Személy- és vagyonvédelmi problémák

A megfigyelő rendszerek felhasználása a személy- és vagyonvédelem területén alapvető biztonsági tevékenységnek számít. A személy- és vagyonvédelem célja az egyén testi épségének, egészségének, biztonságának megóvása, valamint a vagyoni javak (például eszközök, berendezések, készpénz vagy más értékek, akár az üzleti titok) védelme az esetleges károkozással, eltulajdonítással szemben.

A biztonságtechnikai kamerarendszerek helytelen használata azonban pont a célok elérését akadályozhatja, mivel, ha jogosulatlan személyek férhetnek hozzá a megfigyelő rendszerhez vagy a kamerákhoz, azzal a rosszindulatú (akár bűnözési szándékú) elkövetők helyzeti előnyhöz és ártó szándékkal felhasználható információkhoz juthatnak. Nem szabad elfelejteni, hogy a kamerák és megfigyelő rendszerek biztonságtechnikai eszközök, amelyek célja, hogy

---

[17] *A tanulmány csak olyan kameraeszközökkel foglalkozik, amelyek elérhetőek az internet felől, és valamilyen módon lehetőséget biztosítanak a betekintésre*

[18] *https://ipvm.com/reports/aug-13-2019*

megvédjenek bennünket és értékeinket, ezért ezen eszközök biztonsága jelentős kihatással van a személyünkre és védendő értékeinkre.

A célpont felmérése

Egy lakásban vagy családi házban, esetleg az irodaépületekben működő, helytelenül beállított kamerák és kamerarendszerek segítséget nyújthatnak a rosszindulatú elkövetőknek, hogy felmérjék és értékeljék az adott helyszínt.

A kamerák segítségével feltérképezhető, hogy van-e olyan vagyonelem, amelyet érdemes lehet eltulajdonítani. Az is megállapítható, hogy az adott helyszín (lakás, ház, iroda vagy más objektum) mennyire őrzött, hol találhatók esetleg könnyebb behatolási pontok, menekülési útvonalak. Érdemes-e egyedül behatolni, esetleg két emberre, vagy csoportos elkövetésre van szükség a tett sikeres végrehajtásához, például a különféle akadályok leküzdésére, vagy akár a vagyontárgyak elszállításához.

Látható, hogy a kameraképhez vagy videófolyamhoz történő jogosulatlan hozzáférés megkönnyítheti az elkövetők dolgát, és külön szükséges kiemelni, hogy a kamerák helytelen beállítása nagyon könnyen célponttá is teheti a lakókat, vagy egy irodaépület esetén magát az objektumot.

A célpont megfigyelése

Egy családi házban vagy lakásban működő otthonvédelmi, illetve egyéb objektumok fizikai védelmében résztvevő biztonságtechnikai kamerarendszerek esetében a jogosulatlan hozzáférő megismerheti a lakók, tulajdonosok, munkatársak napi rutinját, és a kamerán keresztül megállapíthatja, hogy mikor nem tartózkodnak otthon, vagy a kiszemelt helyiségben, objektumban.

A rosszul beállított vagy sérülékeny kamerák segítségével a megfigyelés távolról megvalósítható, nem szükséges a leendő elkövetőknek a helyszínen tartózkodnia, ezáltal a tevékenység rejtett maradhat. A távoli megfigyelés lehetőséget biztosít a leendő elkövetőnek, hogy akár nagyon hosszú ideig, napokig vagy hetekig figyelje a kiszemelt célpontot, így annak eredménye a napi rutin megállapítása szempontjából sokkal pontosabb, ez pedig lecsökkenti az esetleges lebukás kockázatát.

Irodaépületek vagy egyéb objektumok védelmére gyakran alkalmaznak élőerős őrséget. Ha a leendő elkövető a kamerán vagy kamerákon keresztül követi az őrség mozgását, járőrútvonalakat, váltásokat, ellenőrzési időpontokat, járőrút időtartamokat, akkor kockázatmentesen kiválaszthatja a megfelelő időpontot a behatoláshoz.

Biztonságtechnikai eszközök és eljárások kifigyelése

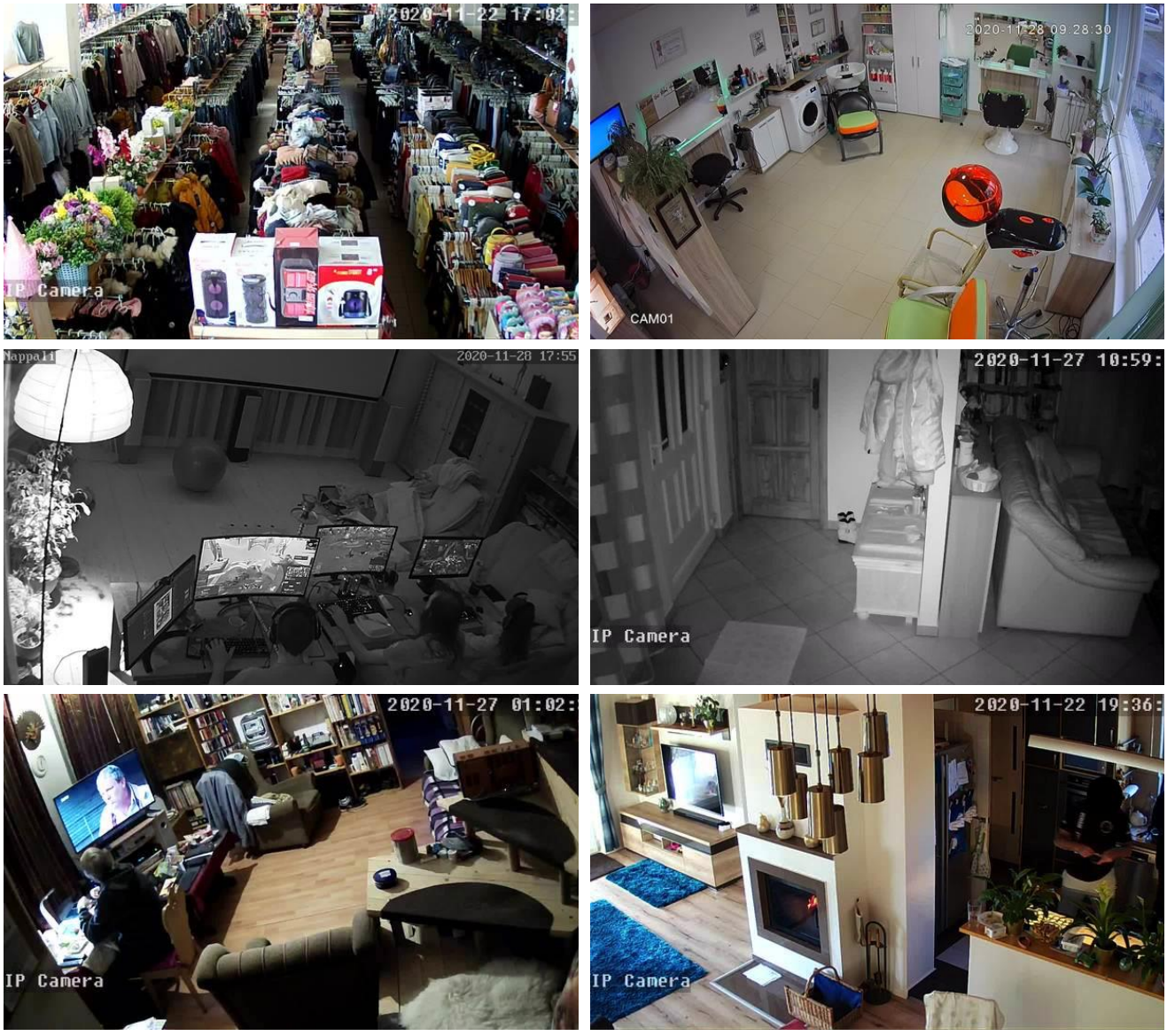
A lakások, családi házak, irodák és egyéb objektumok védelmére a kamerákon kívül egyéb biztonságtechnikai eszközöket is alkalmazhatnak, például beléptető vagy riasztó rendszert, széfeket, páncélszekrényeket, vagy más, mechanikai védelmet.

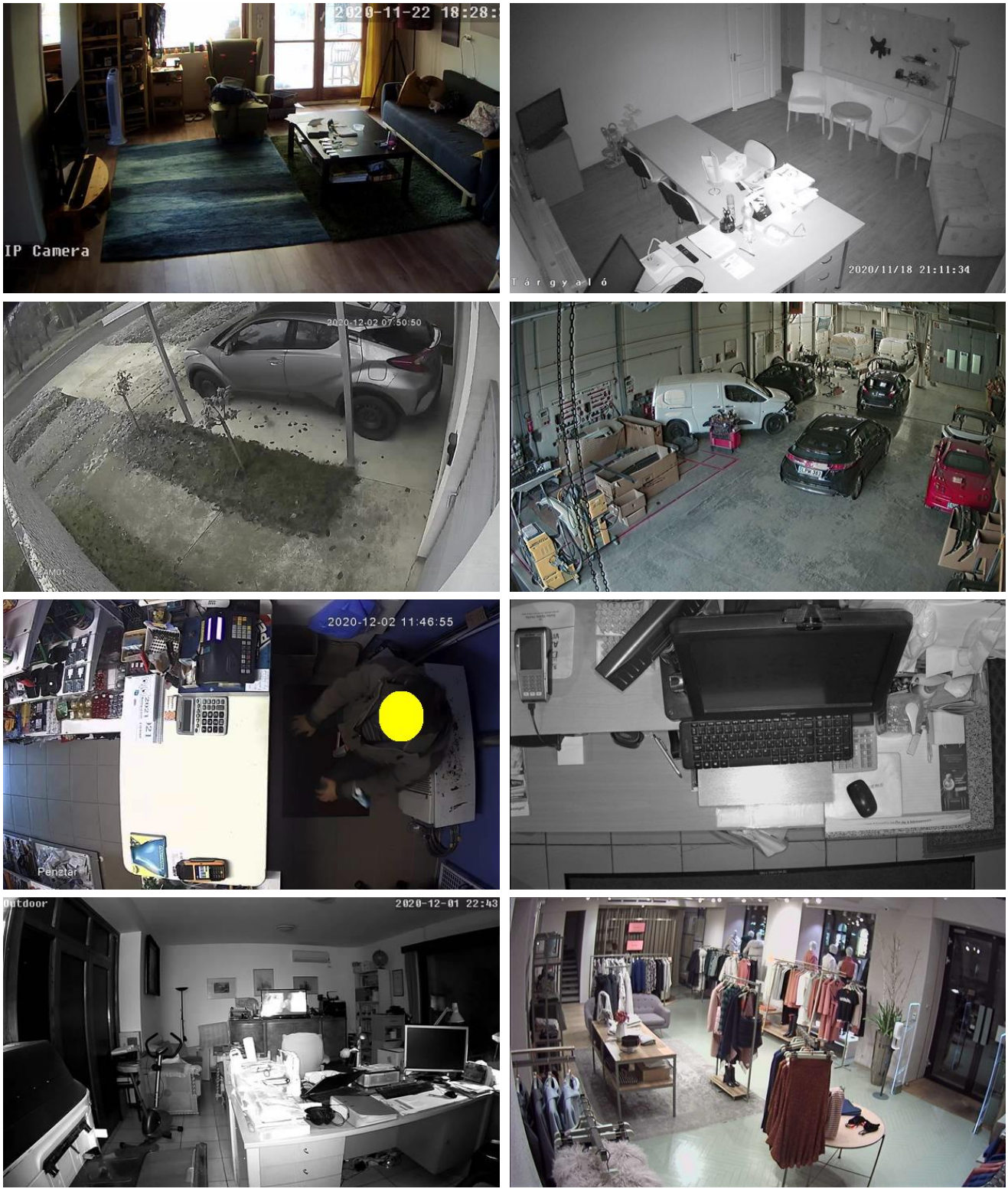
Ha a lehetséges elkövető a rosszul elhelyezett kamerához vagy kamerákhoz hozzáfér, akkor egyszerűen azonosítani tudja a biztonságtechnikai és egyéb védelmi eszközök elhelyezkedését, azaz képes lehet úgy mozogni a terepen, hogy a legkisebb kockázata legyen az észlelésének, illetve az azonosíthatóság és felismerés kockázatát is csökkentheti. Hasonló problémát jelenthet a rosszul elhelyezett és elérhetővé tett biztonsági kamera, ha a bárki számára megtekinthető

kameraképeken, illetve videófolyamban látható a riasztó rendszer (vagy más beléptető) deaktiválása. Ilyen esetekben előfordulhat, hogy a kamerán keresztül a lehetséges elkövető a riasztó kód beütését is követni tudja, azaz képes lesz a riasztót egyszerűen hatástalani. Ugyanez a kockázat merül fel olyan esetekben, amikor biztonsági kamerával követik a széf vagy páncélszekrény nyitását, és valaki jogosulatlanul hozzáfér a kameraképekhez vagy a videófolyamhoz.

Vagyonvédelmi (és természetesen számos adatvédelmi) kockázatot jelenthet például a kasszákhoz telepített, és elérhetővé tett megfigyelőkamera abban az esetben, ha a kamera úgy van beállítva, hogy nem csak a kasszanyitást és zárást rögzíti, hanem akár a bankkártyaterminál használatát, a kártyát és a PIN kód bevitelét. Bár ezt a kockázatot elsősorban az ügyfél viseli, a kamera tulajdonosát is terheli olyan felelősség, amellyel számolnia kell.

Néhány példa az elérhetővé tett hazai biztonsági kamerák világából:





Gyermekvédelmi problémák

A gyermekvédelmi és gyermekjogi kockázatokkal kapcsolatban Dr. Baracsi Katalin családjogi szakjogász és internetjogász nyújtott segítséget.

Számos olyan hazai eszköz található az interneten, amelyek közvetlenül vagy közvetve arra használnak a szülők, hogy gyermekeiket megfigyeljék. A gyermekfigyelésre használt eszközök használata kézenfekvő és rendkívül hasznos, azonban a helytelen beállítások, vagy az esetleges eszköz sérülékenységek miatt az ilyen tevékenység könnyen járhat azzal, hogy maga a gyermek kerülhet veszélybe.

Korábban említésre került az a történet, ahol egy kislányt zaklatott a magát Mikulásnak mondó idegen, de számos további hír vagy figyelmeztetés is található arról, mennyire veszélyessé válhatnak az otthoni megfigyelő, illetve a gyermekek megfigyelésére alkalmazott eszközök.

Egy rochesteri család esetében a gyermekfigyelő monitorjához fért hozzá egy hacker[19], amit csak akkor vettek észre a szülők, amikor az eszköz elkezdett zenélni. A gyermek képeit később egy olyan weboldalon találták meg, amely feltört kamerák képeinek megosztására szakosodott.

Egy másik történetben a bébiszitter a pelenkázáskor hallott hangokat a kamerából[20]. Előbb arra gyanakodott, hogy a szülők viccelik meg, de amikor felhívta őket, kiderült, hogy egy idegen fért hozzá az eszközhöz, aki később a kamerán keresztül dicsérte meg a babát, illetve megjegyzéseket tett a pelenka tartalmára.

Egy houstoni házaspárt és kétéves kislányukat a kamerán keresztül zaklatta egy ismeretlen, akinek sikerült hozzáférnie a gyermekfigyelőhöz[21]. Az illető folyamatosan káromkodott, szidalmazta a gyereket, illetve a házaspárt.

A gyermekek tevékenységét figyelő kamerák jogosulatlan hozzáférése akár veszélyeztetheti is a gyermekek biztonságát. A fentebbi történetek alapján érdemes (bár cseppet sem megnyugtató) abba belegondolni, hogy ha szándékosan vagy akaratlanul is elérhetővé tesszük ezeket az eszközöket, akkor vajon rajtunk kívül ki fogja még a gyermekünket (és bennünket) figyelni, és vajon milyen cselekedetet követhet el az idegen?

A legnagyobb probléma a rosszul beállított vagy megfelelő védelem nélkül elérhetővé tett eszközökkel, hogy célponttá teheti a gyermeket. A gyermekekkel kapcsolatos szexuális bűncselekményeknek a száma évről évre emelkedik, sajnos a névtelenség vélelme és az internet maga is többletlehetőséget biztosít az ilyen cselekmények elkövetésére. Az olyan jelenetek, mint a pelenkázás, meztelenség, intim testrészek látványa, szoptatás, stb. felkeltheti a ragadozók, vagy az őket kiszolgálók érdeklődését, de természetesen az idősebb gyermekek vagy a tinik is könnyen válhatnak célpontokká.

A nemzetközi gyermekvédelem egyik kiemelt szereplője az Inhope[22] szervezet. Az Inhope világméretű, több mint 40 országban tevékenykedő hálózatot működtet, amely célja a gyermekek szexuális kizsákmányolása elleni küzdelem és a gyermekvédelem. Az Inhope a 2019. évi riportjában[23] meglehetősen riasztó tendenciáról számolt be.

---

[19] *https://minnesota.cbslocal.com/2015/04/03/police-baby-monitor-hacked-in-rochester/*

[20] *https://www.krmg.com/news/news/local/man-hacks-baby-monitor-watches-and-talks-babysitte/njzMt/*

[21] *https://abcnews.go.com/blogs/headlines/2013/08/baby-monitor-hacking-alarms-houston-parents/*

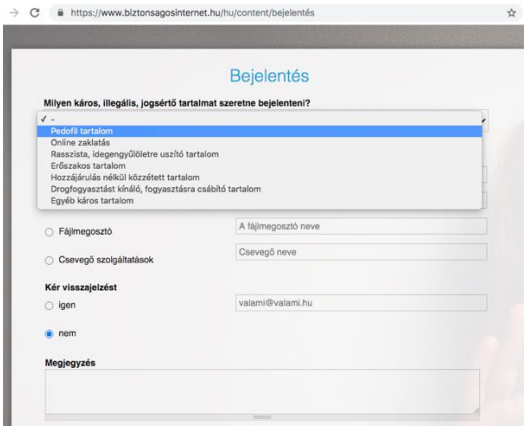
[22] *inhope.org*

[23] *https://inhope.org/media/pages/the-facts/download-our-whitepapers/009c452175-1595854476/annualreport_inhope_2019.pdf*

Míg 2017-ben az Inhope lejelentő rendszerébe 87 930 esemény érkezett, addig a szervezetnek 2019-ben már 183 788 eseményt kellett kezelnie. Tehát megduplázódott azoknak az eseményeknek a száma, amelyben gyermekpornográfiával[24] kapcsolatos tartalmat jelentettek le feléjük, amelyekre reagálva az Inhope elindította a reagálást és a tartalom eltávolítását, illetve megtette a szükséges jogi lépéseket. Az azonosított tartalmak (URL) száma 2019-ben 320 672 volt, a tartalmakban megjelenő gyermekek 92%-a 13 év alatti, a tartalmakban megjelenő gyermekek 91%-a pedig lány.

Az Inhope nem az egyetlen olyan nemzetközi szervezet, amely a gyermekpornográfia ellen küzd, így csak azokról az eseményekről tudnak beszámolni, amelyek hozzájuk kerültek lejelentésre. Okkal feltételezhető tehát, hogy az ilyen tartalmak mennyisége globálisan (az Inhope által regisztrálthoz és lereagálthoz képest) jóval magasabb. Az Internet Watch Foundation szervezet 2019-ben például 260 426 feléjük lejelentett URL-t kezelt a saját rendszerében, amely 2018-hoz képest 25%-os növekedést mutat.

Az Inhope szervezetben Magyarország is képviselteti magát. A Nemzetközi Gyermekmentő Szolgálat Safer Internet Programja, valamint a Nemzeti Média- és Hírközlési Hatóság (NMHH) is tagja a szervezetnek, és hotline-ként képesek eljárni ilyen tartalmak lejelentése esetén. Az NGYSZ Safer Internet Programja egy, az NMHH két elemzővel segíti az Inhope munkáját, ők reagálnak az Inhope által küldött riasztásokra és értesítésekre. Természetesen mindkét hazai szervezet önállóan is végzi a tevékenységet, rendelkeznek saját bejelentő felületekkel (például az NMHH Internet Hotline[25] szolgáltatása), amelyeken jelenteni lehet az ilyen tartalmakat.



A Biztonságosinternet lejelentő felülete
(https://www.biztonsagosinternet.hu/hu/content/bejelentes)

A gyermekek kamerás megfigyelésekor szükséges szem előtt tartani a gyermekjogokat. Az ENSZ közgyűlése 1989-ben fogadta el a Gyermekjogi egyezményt[26], amely összefoglalja azoknak a jogoknak a minimumát, amelyeket minden államnak biztosítania kell a gyermekek számára. Magyarország 1990-ben írta alá az egyezményt, amelyet az 1991. évi LXIV. Törvényben hirdetett ki.

---

[24] *Az Inhope terminológiája a Child Sexual Abuse Material megnevezést, azaz a CSAM rövidítést használja.*

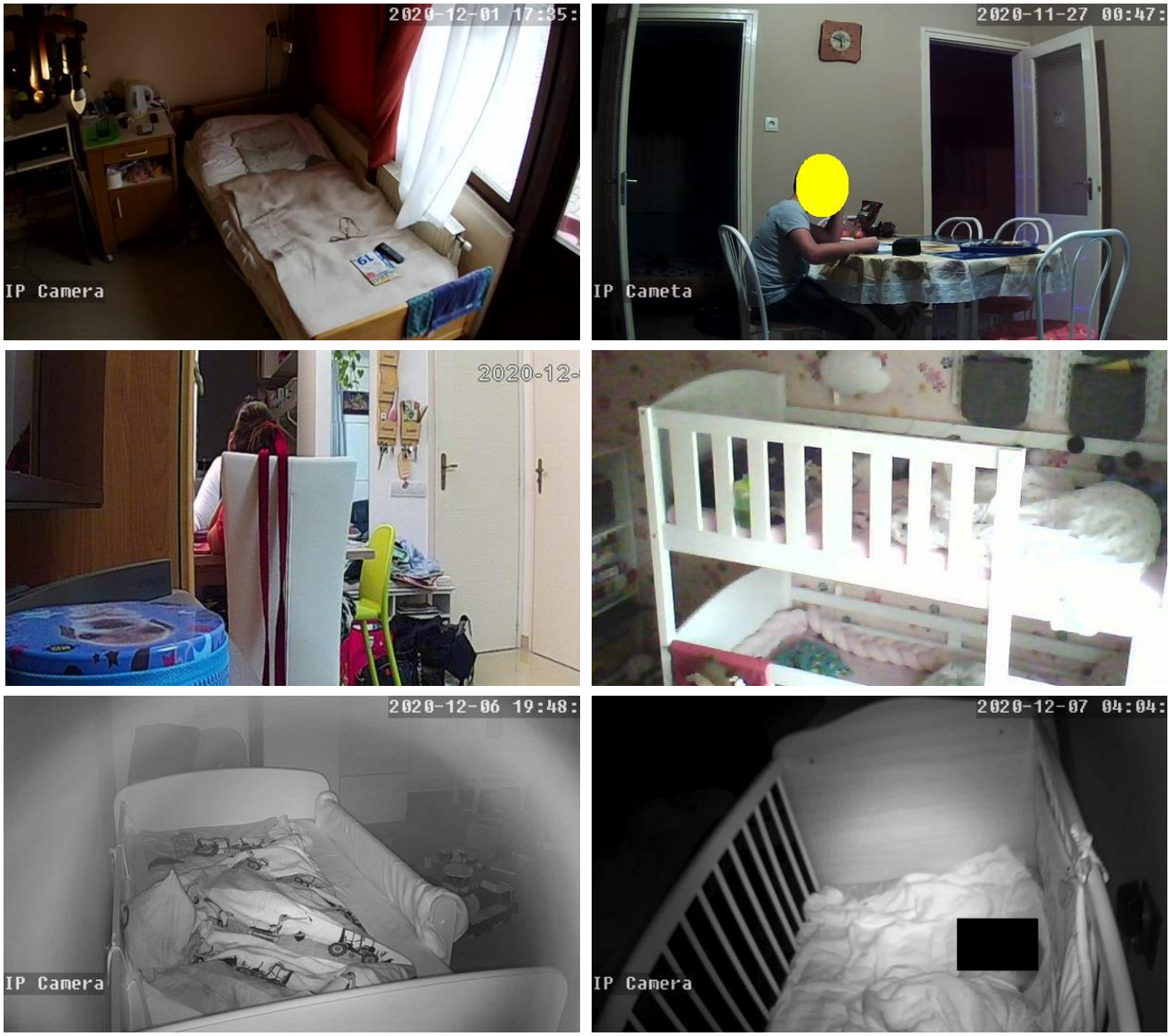
[25] *https://nmhh.hu/internethotline/*

[26] *https://unicef.hu/gyermekjogok*

Bármennyire jószándékból és szülői gondoskodásból fakad a gyermek kamerás megfigyelése, figyelemmel kell lenni a gyermek magánélethez való jogára is (16. cikk). A gyermeket megilleti a védelem az erőszak (19. cikk), valamint a szexuális kizsákmányolás minden formájától (34. cikk). A legnagyobb jószándékkal telepített kamerához jogosulatlanul hozzáférő személy fenyegetést jelenthet a gyermekre, illetve a gyermek jogaira, hiszen egy akaratlanul, bárki számára elérhetővé tett megfigyelőkamera is kiteheti a gyermeket erőszaknak, szexuális kizsákmányolásnak, zaklatásnak, megfélemlítésnek, fenyegetésnek, vagy egyéb veszélyeknek.

Dr. Baracsi Katalin szerint a gyermekek magánélethez való joga mellett a gyermek tájékoztatáshoz való joga (17. cikk) is sérülhet, ha a kamerás megfigyelésről a szülők nem tájékoztatják. Súlyos bizalomvesztés is felléphet a szülővel szemben, ha a gyermek számára kiderül, hogy a szülei megfigyelték a tevékenységét. Az életkorának megfelelően szükséges tájékoztatni a gyermeket, hogy a biztonsága érdekében technikai eszközzel figyelik meg a szobáját, vagy más olyan helyiségeket, ahol tevékenykedik. A technikai eszközök segítségével a szülő könnyebben tudhatja biztonságban a gyermekét, azonban ez nem mehet a gyermekjogok rovására.

Néhány „elrettentő” példa az elérhetővé tett gyermekmegfigyelő kamerák világából



Adatvédelmi problémák

A GDPR hatályba lépése (2016) és alkalmazandóvá válása (2018) óta az adatvédelmi előírások jelentősen szigorodtak. A kamerás megfigyelésre vonatkozó szabályok figyelmen kívül hagyása akár adatvédelmi bírságot is eredményezhet, így a kamerák telepítésénél és beüzemelésénél érdemes figyelembe venni a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) és a hatályos hazai jogszabályok vonatkozó ajánlásait, illetve rendelkezéseit.

A kamerák munkahelyi használatára és a munkatársak kamerával történő ellenőrzésére vonatkozó adatvédelmi elvárások összefoglalásában és értelmezésében a Holló Ügyvédi Iroda[27] vezetője, Dr. Holló Dóra nyújtott adatvédelmi jogi segítséget a tanulmány megírásához.

[27] *http://hplaw.hu/*

Maga a GDPR nem tartalmaz kifejezett rendelkezéseket a kamerarendszer üzemeltetésével vagy a munkavállalók kamerás megfigyelésével kapcsolatban. A munkavállalók személyes adatainak kezelésére vonatkozóan a GDPR (155) preambulumbekezdése, illetve 88. cikke úgy rendelkezik, hogy ebben a kérdésben a tagállamok jogszabályban vagy kollektív szerződésekben pontosabban meghatározott szabályokat állapíthatnak meg – így történik ez a magyar jogrendszerben is.

A GDPR tehát csak általános jelleggel állapít meg a személyes adatok kezelésére vonatkozó szabályokat. A munkavállalók kamerás megfigyelésére vonatkozó előírások megismeréséhez azonban a kapcsolódó magyar jogszabályokat kell megvizsgálni.

A tanulmányban bemutatott és azonosíthatóan munkahelyi, közösségi (vagy a plázák és boltok esetében a vásárlói) tér megfigyelésre használt, illetve a bárki számára betekinthetővé tett kamerák esetében az értékeléshez egyrészt a GDPR általános rendelkezései szintjén, másrészt pedig a munkavállalói adatok kezelésére, illetve kamerás megfigyelésre vonatkozó magyar ágazati jogszabályok szintjén kellett vizsgálódni. Figyelembe vettük továbbá a NAIH állásfoglalásait, tájékoztatóit, illetve eljárási gyakorlatát is.

A GDPR 5. cikke meghatározza azokat a személyes adatok kezelésére vonatkozó alapvető követelményeket, amelyeknek a személyes adatok gyűjtése és kezelése során érvényesülnie kell, a 6. cikke pedig meghatározza azokat a feltételeket, amelyek valamelyikének fennállása esetén a személyes adatok jogszerűen kezelhetők (ezek a „jogalapok").

Nehéz elképzelni olyan körülményt, amelynek fennállása esetén a 6. cikk szerinti jogalapok valamelyike megállna egy ilyen, az érintettek alapvető személyiségi jogait durván sértő adatkezelés folyamán. Viszont még ha a jogalap meg is van az adatkezeléshez, ugyanilyen nehéz elképzelni, hogy az 5. cikk szerinti minimumkövetelmények ne sérülnének (például jogszerűség, célhoz kötöttség, adattakarékosság, korlátozott tárolhatóság, integritás és bizalmas jelleg, hogy csak a legnyilvánvalóbbak kerüljenek említésre).

Ha a nyilvánosan elérhető, bárki számára betekinthetővé tett kamerák kérdése nem csak a GDPR általános szintjén vizsgált, hanem a munkavállalói adatok kezelésére, illetve a kamerás megfigyelés szabályaira vetítve is, akkor megállapítható, hogy egy ilyen típusú adatkezelés szinte biztosan az irányadó magyar jogszabályokba ütközik:

- A munka törvénykönyvéről szóló 2012. évi I. Törvény (Mt.) 11/A. §-a rendelkezik a munkavállalók ellenőrzéséről, amelynek (1) bekezdése kimondja, hogy a munkavállaló csak a munkaviszonnyal összefüggő magatartása körében ellenőrizhető, és technikai eszközzel csak akkor, ha a munkáltató előzetesen írásban tájékoztatja erről.
- Az Mt. ezen rendelkezését a NAIH munkahelyi adatkezelések alapvető követelményeiről szóló tájékoztatója, illetve a munkahelyen alkalmazott elektronikus megfigyelőrendszer alapvető követelményeiről szóló ajánlása egyértelművé teszik, hogy a munkavállaló önkéntes hozzájárulása a munkaviszony keretei között a két fél között fennálló hatalmi viszony miatt csak nagyon szűken értelmezhető és alkalmazható jogalap, tehát ebben az esetben csakis a munkáltató jogos érdeke jöhet szóba.
- Vannak olyan további garanciális szabályok, amelyek a munkáltató mozgásterét szűkítik; példaként idézve a NAIH munkahelyi adatkezelésekre vonatkozó tájékoztatójából:

„Az elektronikus megfigyelőrendszerek alkalmazhatóságának fontos feltétele, hogy semmiképp sem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzókban, az illemhelyiségekben vagy például orvosi szobában, váróban. Emellett alapvetően szintén nem lehet elektronikus megfigyelőrendszert alkalmazni az olyan helyiségben sem, amely a munkavállalók munkaközi szünetének eltöltése céljából lett kijelölve, mint például a munkavállalók számára biztosított ebédlő. Ez alól kivételt jelenthet az az esetkör, ha ebben a helyiségben valamilyen védendő vagyontárgy található (így például étel-ital automata), amellyel összefüggésben igazolható valamilyen munkáltatói érdek (például a munkavállalók többször megrongálták a berendezést és a károkat a munkáltatónak kellett állnia). Ebben az esetben e konkrét cél érdekében kamera helyezhető el a helyiségben, azonban ekkor a munkáltatónak különös figyelemmel kell lennie arra, hogy a kamera látószöge kizárólag a védendő vagyontárgyra irányulhat. A kamerák látószögével kapcsolatban fontos megjegyezni, hogy a munkáltató elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhat, közterület megfigyelésére azonban nem.”

- A személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény (Szvtv.) 30. § (2) bekezdése kimondja továbbá, hogy nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti. A 31. § pedig úgy rendelkezik, hogy az elektronikus megfigyelőrendszer működése útján rögzített kép- és hangfelvétel megismerésének okát és idejét, valamint a megismerő személyét jegyzőkönyvben kell rögzíteni. Egy interneten keresztül megosztott és bárki számára megismerhetővé tett kamerafelvétel esetén ez a feltétel nyilvánvalóan nem tud teljesülni, tehát a munkavállalók megfigyelését nyilvánossá tenni a hatályos magyar jogszabályok szerint egyértelműen nem jogszerű. Az idézett jogszabályi rendelkezés egyébként nem csak a munkavállalók kamerás megfigyelése tekintetében alkalmazandó, hanem irányadó bármilyen, magánterületen alkalmazott megfigyelőrendszer alkalmazásában.
- Kijelenthető tehát, hogy a kamerafelvételek bárki számára nyilvánossá tétele nem csak a munkavállalók megfigyelése tekintetében ütközik az Szvtv.-be, hanem ugyanígy sérti bármilyen, a felvételeken szereplő személy (például a vásárlók) jogait is.

Ha nem kifejezetten csak a munkavállalók, hanem bármely, a kamerák látószögébe kerülő személy szempontjából vizsgáljuk a kérdést, akkor ugyanígy igazak a GDPR általános szabályai körében tett megállapítások (tehát a GDPR a kamerás megfigyelésre vonatkozóan nem állapít meg konkrét szabályokat), azonban, ahogy korábban kifejtésre került, a magyar jogszabályok szintjén ez a gyakorlat biztosan a Szvtv. idézett rendelkezéseibe ütközik.

E körben megemlítendő továbbá a Polgári törvénykönyvről szóló 2013. évi V. törvény (Ptk.) 2:43. §-a, amely szerint a képmáshoz való jog megsértése a személyiségi jogok sérelmével jár. A gyakorlatban ez azt jelenti, hogy egy jogosulatlanul készített felvétel, illetve annak nyilvánossá tétele nem csak az adatvédelmi vonatkozású jogszabályokat, hanem az érintett személyiségi jogait is sérti, amely esetben a Ptk.-ban ilyen esetekre megállapított szankciók alkalmazhatóak a jogsértővel szemben (pl. sérelemdíj vagy kártérítés követelése).

A fentiek alapján megállapítható, hogy a GDPR általános jelleggel állapít meg szabályokat az adatkezelés jogszerűségére vonatkozóan, explicite nem zárja ki a munkavállalók vagy például a

vásárlók kamerás megfigyelését, illetve ezen felvételek nyilvánossá tételét. Elméletileg tehát bármilyen adatkezelési gyakorlat jogszerű lehet, ha az a GDPR 5. cikkében meghatározott minimumkövetelményeknek megfelel, ha a GDPR 6. cikke szerinti valamely jogalappal igazolható, és teljesülnek rá a GDPR 7-23. cikkében foglalt további követelmények, amelyek az érintettek tájékoztatását, illetve jogaik védelmét szolgálják. A hangsúly itt azonban az „elméletileg" kifejezésen van, hiszen gyakorlatilag szinte lehetetlen elképzelni olyan szituációt, amelyben a munkáltató, vagy a kamera működtetőjének jogos érdeke igazolhatná azt, hogy a munkavállalókról vagy vásárlókról készült felvételeket bárki megismerhesse, és az e körben elvégzett érdekmérlegelési teszt eredményeképp a munkáltató, vagy a kamera működtetőjének érdeke előnyt élvezhetne a munkavállaló, illetve vásárló alapvető jogaival, méltóságával szemben.

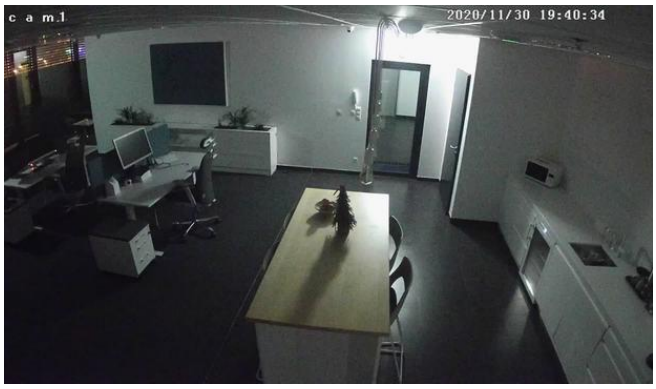
Ha nyilvánosan elérhetővé tett munkahelyi megfigyelőkamerák helyzete az ágazati magyar jogszabályok, illetve a NAIH gyakorlatának szintjén vizsgált, akkor megállapítható, hogy ez az adatkezelés a magyar jog szerint egyértelműen jogellenes, mivel több ponton is sérülnek az Mt.-ben (és ezzel összefüggésben a NAIH által kiadott anyagokban), valamint az Szvtv.-ben meghatározott követelmények.

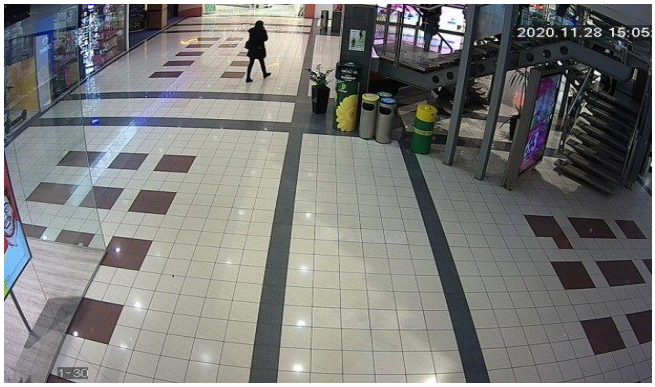
A nem megfelelő jogalappal végzett adatkezelés, illetve az érintettek alapvető jogainak megsértésének esetére a bírság maximális összege a GDPR 83. cikkének (5) bekezdése alapján legfeljebb 20 000 000 EUR összegű közigazgatási bírság, illetve a vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4 %-át kitevő összeg, azzal, hogy a kettő közül a magasabb összeget kell kiszabni. A GDPR alkalmazandóvá válása óta eltelt években több, jogszerűtlen kamerás megfigyeléssel kapcsolatos bírságot is kiszabott a Nemzeti Adatvédelmi és Információszabadság Hatóság, azonban ezek általában 500.000,- Ft és 1.000.000,- Ft közötti összegek voltak.

Néhány példa az elérhetővé tett munkahelyi megfigyelő kamerák világából


2020.12.03 16:52
2-27


Tárgyaló
2020/11/18 21:11:34

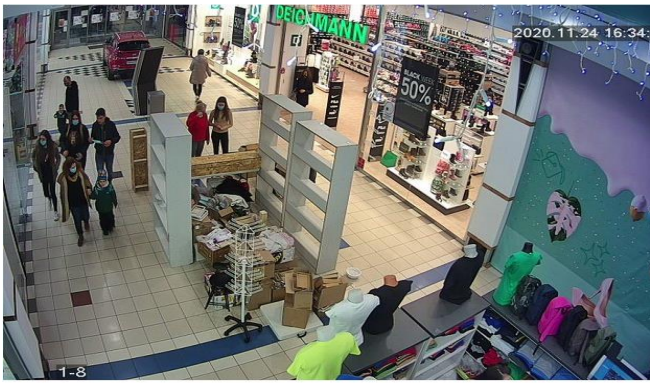

cam1
2020/11/30 19:40:34


2020.11.28 15:05


VISION EXPRESS
2020-12-05 03:25
KECSKEMÉT LINARTECH
1-4


2020-12-01 20:28:
IP Camera


CAM01


DEICHMANN
50%
2020.11.24 16:34
1-8


2020/12/08 06:03:38


H&M
2020.12.04 08:14
2-06


2020-12-09 13:26:42
CAM01


2020-12-10 Thu 21:34:14
Camera 01

Biztonsági javaslatok vállalati célra felhasznált eszközök esetén

Beszerzéskor

Alapos, megfontolt kiválasztás

A vállalati célra felhasznált eszközök beszerzésekor kiemelt gondossággal javasolt eljárni. Az eszközök részeivé válnak a vállalati hálózatnak, így az egyenszilárdságú biztonság érdekében a megfigyelő, illetve rögzítő eszközöknek teljesíteniük kell azokat a biztonsági elvárásokat, amelyek szavatolják, hogy az eszközök nem jelentenek kockázatot a vállalati hálózat és a felhasználók számára. Beszerzéskor sok esetben az eszközök ára számít a legfontosabb döntési tényezőnek, azonban ez súlyosan fenyegetheti a hálózat és a felhasználók biztonságát. Fontos, hogy a biztonsági szempontok is hangsúlyt kapjanak a beszerzési eljárásokban.

Feltűnően olcsó kamerák kerülése

Nem állítható, hogy minden, az Aliexpressen és a hasonló oldalakon értékesítésre kínált, pl. kínai gyártmányú kameraeszköz veszélyes, azonban korábban is említésre került, hogy a különféle OEM licenszelt eszközök esetében nem igazán tudható, hogy pontosan ki a gyártó, kihez lehet fordulni, vagy ki a felelős a termék minőségéért. Ebből kiindulva abban sem lehetünk biztosak, hogy betartották-e a biztonsági követelményekre vonatkozó szabványokat, elvárásokat vagy ajánlásokat. A rebrandelt, OEM licenszelt eszközök esetében az is problémát jelenthet, hogy sok esetben egyáltalán nem is lehet kapcsolatba lépni a „gyártóval”, így sem információt, sem pedig javításokat nem lehet beszerezni. Az utóbbi években több, rendkívül súlyos sérülékenység köthető az ilyen eszközökhöz, de természetesen a magasabb árú, esetleg ismert gyártóktól származó eszközök biztonsági állapota is hagyhat kivetnivalót maga után, így a következő pont figyelembevételével érdemes döntést hozni a kérdésben.

Ismeretlen gyártótól származó eszközök kerülése

Az előző pontban, a feltűnően olcsó eszközök esetében is említésre került, hogy nagyon sok átcímkézett és átmárkázott termék található a piacon, amelyek esetében sejtelmünk sincs arról, hogy valójában ki a gyártó. Amennyiben egy vállalat figyelembe veszi a biztonsági szempontokat, javasolt olyan megbízható forrásból és gyártótól beszerezni az eszközöket, amelyek ismertek a piacon, és amelyeknél rendelkezésre állnak hiteles értékelések, vagy például valós tesztesetek, valamint elérhetők a frissítések, javítások.

Kiválasztott gyártó és eszköz ellenőrzése

Amikor kiválasztásra kerül egy megoldás, javasolt alaposan utánanézni az eszközzel és gyártójával kapcsolatos tapasztalatoknak. Érdemes ellenőrizni a gyártóval és eszközeivel kapcsolatos ismert sérülékenységeket, illetve a sérülékenységi listák alapján megvizsgálni például a biztonsági javítások kiadásával kapcsolatos idővonalakat. Ha egy gyártó a lejelentett és igazolt sérülékenységekre nem ad ki javítást, vagy láthatóan nagyon lassú a reagálása, akkor abból már következtetéseket lehet levonni a biztonsággal kapcsolatos hozzáállásáról. A biztonságot komolyan vevő gyártók gyakran adnak ki „*hardening guide*" dokumentációt, amely bemutatja, hogyan kell az eszközt biztonságosan beállítani és használni. Az ilyen dokumentum jelentős segítséget nyújt a vállalat számára szükséges és elvárt biztonsági funkciók beállításában és alkalmazásában.

Biztonsági funkciók ellenőrzése

Érdemes megvizsgálni, hogy milyen funkciók találhatók az eszközben, amelyek alkalmazása szavatolni tudja, hogy az eszköz megfelelően integrálható a vállalati hálózatba és nem válik esetleg olyan kockázattá, amellyel egyébként nem lenne tisztában a működtető. Általános elv, hogy a hálózat védelme csak annyira erős, mint a hálózatban működő legvédtelenebb eszköz, így az eszköz biztonsági funkcióit a hálózatvédelem képességeihez és elvárásaihoz képest szükséges ellenőrizni, majd illeszteni.

Beüzemeléskor

A dokumentációk alapos áttanulmányozása

Legyen szó a beüzemelési, vagy akár a *hardening guide* dokumentumról, a dokumentációk áttanulmányozása és az azokban foglaltak alkalmazása nagyban elősegíti, hogy a kamera vagy más rögzítő eszköz biztonságosan üzemeljen. Triviálisnak hangzik, de a dokumentáció és a benne szereplő módszerek, eljárások, javaslatok és figyelmeztetések figyelmen kívül hagyása nagyon könnyen vezethet hibás integrációhoz és biztonsági kockázatokhoz. Javasolt, hogy ha az adott eszköz rendelkezik *hardening guide* dokumentációval, akkor a beállítás során a dokumentum alapján járjon el a telepítő személy.

Szegmentáció, szeparáció

A vállalati környezetekben javasolt, hogy az IoT eszközök (és így a különféle megfigyelő vagy rögzítő eszközök is) egy, a vállalati hálózattól elkülönített, és határvédelmi eszközzel (tűzfal), vagy legalább logikai szeparációval (például VLAN) elválasztott zónába kerüljenek telepítésre. Az egyes hálózati zónák eszközei eltérő biztonsági szintekkel és elvárásokkal rendelkezhetnek. A szeparáció biztosítani tudja, hogy egy alacsonyabb biztonsági képességű eszköz esetleges sérülékenysége ne okozzon problémát és kockázatot a teljes vállalati hálózat számára, ne fenyegethesse a vállalati hálózat, a benne található eszközök és a felhasználók biztonságát.

Biztonságos hálózati kapcsolat

Főleg a wifi-képes eszközök esetén kiemelt fontosságú (de a kábeles csatlakozások esetében is), hogy az átviteli hálózat képes legyen garantálni az eszköz, illetve az adatok bizalmasságát, sértetlenségét és rendelkezésre állását. A modernebb kamerák támogatják az eszközök hálózati hitelesítését, így javasolt, hogy a wifi hálózat WPA2-Enterprise (802.1x) hitelesítési eljárást

alkalmazzon. Amennyiben erre nincs lehetőség, a WPA2-PSK csatlakozás mellett javasolt legalább az eszközök egyedi MAC címéhez kötni a hálózati kapcsolat engedélyezését.

Kamerahálózat elérésének korlátozása

Ha a megfigyelő és rögzítő eszközök a vállalati hálózattól elkülönített zónában működnek, javasolt korlátozni a hálózatok közötti átjárást. Csak olyan hálózatból szabad elérhetővé tenni ezeket az eszközöket, amelyek megbízhatók, illetve csak azok számára, akiknek erre a szolgáltatásra szükségük van. Ezzel együtt javasolt, hogy a kamerákat és rögzítő berendezéseket az internet felől közvetlenül egyáltalán ne lehessen elérni.

Legfrissebb firmware verzió használata

A telepítéskor javasolt az eszközök operációs rendszerét (*firmware*) a lehető legújabbra frissíteni, ezáltal az eszközök korábbi, esetleges biztonsági hibái javításra kerülhetnek. A frissítés ebből a szempontból egy kritikus tevékenység, az eszközök üzemeltetésekor tehát törekedni kell arra, hogy időközönként ellenőrzésre kerüljenek a verziók, és ha megjelent újabb frissítés, akkor azt telepíteni kell.

Megbízható firmware és operációs rendszer használata

Csak megbízható forrásból, például a gyártói oldalról letöltött firmware vagy javítás telepítendő. A biztonságot fontos területként kezelő gyártók digitálisan aláírják a firmware vagy frissítési csomagokat, ez elviekben garantálja, hogy azokba a gyártó tudtán kívül nem nyúlt bele senki és nem helyezett el benne például kártékony kódot, vagy backdoort. A letöltés után javasolt a csomag digitális aláírását ellenőrizni, hogy meggyőződhessünk arról, sem a gyártói oldalon, sem a letöltéskor nem sérült a csomag integritása. Éles környezetekben *early* vagy *beta* verziók használata nem javasolt, mivel ezekben még maradhattak olyan hibák, amelyeket a minőségellenőrzés (ha van) nem vett észre és amelyek kockázatot jelenthetnek.

Kliens alkalmazás frissítése a legújabb verzióra

Telepítéskor érdemes mindig a legújabb verziót telepíteni, azonban, ha az integráció során egy régebbi kliens alkalmazást telepítettek, javasolt azt frissíteni a legújabb verzióra. Egy megfigyelő vagy rögzítő rendszer kliens oldali komponense is tartalmazhat sérülékenységeket vagy biztonsági hiányosságokat, így hasonlóan a firmware frissítéshez, a legújabb verzió használatával a korábbi verziók sérülékenysége is javítható.

A gyártótól származó kliens alkalmazás használata

Sok eszköz lehetővé teszi, hogy szabványos kapcsolatokon keresztül akár idegen gyártótól vagy fejlesztőtől származó kliens alkalmazással (például stream néző vagy rendező, felügyeleti alkalmazások, stb.) csatlakozni lehessen a megfigyelő vagy rögzítő eszközökhöz. Javasolt azonban mindig a kamera vagy rögzítő gyártójától származó, vagy az általuk ajánlott megoldást alkalmazni, mivel ezeknél kisebb lehet az esetleges interoperabilitásból származó probléma vagy sérülékenység bekövetkezése. Az is fontos szempont, hogy egyszerűbb naprakészen tartani a homogén rendszereket, hatékonyabban lehet például a frissítéseket és javításokat telepíteni.

Alapértelmezett jelszavak megváltoztatása

Sajnos nagyon sok eszköz alapértelmezett felhasználói hozzáférésekkel érkezik, amelyeket a telepítés végén néha elfelejtenek megváltoztatni. Több olyan oldal is elérhető az interneten, ahol

a megfigyelőeszközök alapértelmezett hozzáféréseit gyűjtik össze[28]. Az érintetlenül hagyott alapértelmezett hozzáférések lehetőséget adhatnak jogosulatlan személyeknek arra, hogy hozzáférjenek a kameraképekhez, videófolyamokhoz, illetve az eszközök beállításaihoz. Javasolt a telepítéskor azonnal lecserélni az alapértelmezett jelszavakat és kellően biztonságos jelszavakat beállítani.

Az alapértelmezett felhasználók letiltása

Amennyiben erre az eszköz lehetőséget ad, javasolt az eszközzel érkező összes gyári felhasználói hozzáférést letiltani. A *XiongMai* eszközök esetében a gyártó XMEye P2P Cloud szolgáltatásnak minden eszközön létezett egy alapértelmezett felhasználója (*admin/üres jelszó*) amely miatt, ha a hozzáférés nem került letiltásra, vagy a jelszó megváltoztatásra, a támadók csatlakozhattak a kamerákhoz. Alapvető biztonsági elvárás, hogy az olyan hozzáférések, amelyeket nem használnak (vagy nem tudják mire is szolgál), kerüljenek letiltásra, illetve lehetőség szerint egyetlen, az eszközzel érkező hozzáférés se maradjon aktív a rendszerben. A legbiztonságosabb, ha az igényeknek megfelelően a tulajdonos vagy üzemeltető egyedi, a felhasználókhoz dedikált, nevesített és funkciókhoz kötött hozzáféréseket hoz létre és ellátja azokat a megfelelő, biztonságos jelszavakkal.

A nem használt felhasználók letiltása

Az előző ponthoz is tartozik, de külön is ki kell emelni, hogy csak olyan hozzáférések legyenek létrehozva a rendszerben, amelyek valóban használva is vannak, és amelyekre a működéshez, illetve működtetéshez szükség van. Sok esetben elmaradhat például egy olyan felhasználó törlése, aki már nem dolgozik a vállalatnál, vagy egyéb okból megvonásra került a hozzáférési jogosultsága. Biztonsági szempontból az adminisztratívan visszavont, de a valóságban nem letiltott vagy nem törölt felhasználó jogosulatlan hozzáférési lehetőséget jelent. Periodikusan érdemes a rendszert felülvizsgálni, és a felesleges felhasználói hozzáféréseket letiltani vagy törölni.

Felhasználónév és jelszó beállítása a menedzsment felület eléréséhez

Célszerű a menedzsment felülethez való hozzáférést és a felhasználói videófolyam hozzáféréseket elválasztani egymástól. Javasolt szerepkörökben gondolkodni, és a funkcionalitáshoz kötötten létrehozni a hozzáféréseket, valamint beállítani a jogosultságokat. Például a menedzsment felületet elérő felhasználók csak a menedzsment felületet és beállításokat érhessék el és ne legyenek képesek az élő képet, videófolyamot vagy a rögzítéseket megnézni és visszanézni. Érdemes a szerepkörök kialakításához adatvédelmi szakértővel, vagy a vállalat adatvédelmi tisztviselőjével (DPO) konzultálni, hogy a kialakított szerepkörök és jogosultságok megegyezzenek a kamera szabályzatban foglaltakkal, illetve biztosított legyen az adatvédelmi megfelelőség.

Felhasználónevek és jelszavak létrehozása a kliensekhez, streaming alkalmazásokhoz

Amennyiben lehetőség van a szerepkörök szétválasztására és a szofisztikáltabb jogosultságkiosztásra, javasolt, hogy a felhasználóknak a menedzsmenttől eltérő, egyedi, nevesített hozzáférések kerüljenek létrehozásra úgy, hogy semmilyen menedzsment vagy adminisztratív funkciót ne érhessenek el. Javasolt, hogy a különféle klienseknek vagy kliens

[28] *Például: https://learncctv.com/ip-camera-default-password/*

alkalmazásoknak legyen egyedi, azonosítható hozzáférés kialakítva, a lehető legszűkebb, csak a működéshez (például adatfolyam elérés) szükséges jogosultsággal.

Egyedi, megfelelően erős jelszavak használata

A létrehozott felhasználói, technikai (pl. streaming alkalmazás) és adminisztratív hozzáférésekhez egyedi és biztonságos jelszavak kerüljenek beállításra. Ügyelni kell arra, hogy egyetlen hozzáférés se használjon olyan jelszót, amelyet esetleg egy másik hozzáférés használ. A jelszavak újra felhasználása („*password reuse*") nagyban megkönnyítheti egy támadó dolgát, ha egy esetleg kompromittált jelszóval akár felhasználó, vagy adminisztrátor nevében is be tud jelentkezni. Ugyancsak érdemes a jelszavak létrehozásakor figyelemmel lenni a vállalat jelszavakkal kapcsolatos utasításaira és elvárásaira. Kerülni kell továbbá a kitalálható vagy alacsony bonyolultságú, ezért könnyen megfejthető jelszavak használatát.

Titkosítatlan kommunikáció (pl. HTTP, Telnet, FTP) letiltása

A HTTP és más, titkosítatlan kommunikációs lehetőségeket javasolt letiltani és helyettük a titkosítással rendelkező változatot beállítani, illetve használni, például HTTP helyett HTTPS, Telnet helyett SSH, FTP helyett SFTP szolgáltatásokat bekapcsolni. A titkosítatlan kommunikáció lehetővé teszi, hogy egy megbízhatatlan hálózati kapcsolódás során (például idegen hálózat, nyilvános wifi, stb) a forgalmat lehallgassák és megszerezzék a hozzáféréshez szükséges felhasználóneveket és jelszavakat. Ez nemcsak a kamerák vagy rögzítők elérése során fontos, hanem igaz az olyan kapcsolatokra is, amelyet maguk az eszközök indítanak, például amikor egy kamera állapotképeket tölt fel egy másik hálózatban működő, vagy akár az interneten elérhető szerverre (FTP). Ha a kamera képes rá, a videófolyam továbbítás során az adatforgalmat is titkosítani kell (Secure RTP).

Saját, megbízható tanúsítványok használata (SSL/TLS)

Javasolt az eszköz gyári SSL/TLS tanúsítványait saját, megbízható tanúsítványokra cserélni. A saját tanúsítványok használata segíthet a felhasználóknak meggyőződni arról (például webes kapcsolat során), hogy a kapcsolat valóban megbízható és a forgalmat – jó eséllyel- nem hallgatja le egy idegen személy. Gyakorlatilag a megbízható tanúsítványok a kapcsolat és az adatforgalom integritásának védelmét és ellenőrizhetőségét szolgálják.

Felhős kapcsolatok ellenőrzése, lehetőség szerint letiltása

A megfigyelőkamerák biztonsági eszközök, így a lehető legtöbbet meg kell tenni annak érdekében, hogy működésük ellenőrizhető, átlátható és biztonságos legyen. A felhős menedzselésű, vagy felhőn elérhető kamerák esetében számos olyan sérülékenység vagy probléma előfordulhat, amely kockázatot jelenthet a vállalat részére. A *XiongMai* és eszközváltozatai esetében a felhős kapcsolat jelentette azt a sérülékenységet, amely miatt sokezer kamera kompromittálódott. Érdemes kijelenteni, hogy a felhő nem ellenség, azonban csak abban az esetben szabad használni, ha pontosan tudjuk mit várhatunk tőle. A biztonsági eszközöket, például a kamerákat lehetőség szerint nem a felhőn, hanem egy biztonságos VPN kapcsolaton javasolt elérhetővé tenni.

P2P funkció használatának kerülése, lehetőség szerint letiltása

A felhős kapcsolat használatának letiltásához kapcsolódik a különféle P2P szolgáltatások tiltása. A P2P segítségével lehet a felhőn keresztül elérhetővé tenni az eszközöket, azonban

korábban több ilyen megvalósítás gyenge biztonsági szint mellett történt. 2017-ben olyan P2P-hez köthető sérülékenység jelent meg, amely 1253 különféle kameratípust[29] érintett. Akkor több mint 185 000 olyan kameraeszköz vált kompromittálhatóvá a sérülékenység miatt, amelyek elérhetők voltak az internet felől. Jelen pillanatban „csak" 41 ezer eszközt talál a Shodan eszközkereső[30], amely ebből a szempontból még sérülékeny lehet. A biztonsági eszközöket - például a kamerákat- nem a felhőn, hanem egy biztonságos VPN kapcsolaton keresztül javasolt elérhetővé tenni, amennyiben ez lehetséges.

UPnP szolgáltatás letiltása

Az UPnP szolgáltatás segítségével az eszközök és a routerek emberi beavatkozás nélkül képesek egyeztetni és engedélyezni azokat a kommunikációs portokat, amelyekre az eszközöknek szüksége lehet a működéshez. Komoly problémát jelent, hogy az eszköz az UPnP protokollon keresztül képes jelezni a routernek, hogy az engedélyezze az internet felől az eszközhozzáférést, azonban a tulajdonosnak gyakran nincs is tudomása arról, hogy online elérhetővé vált az eszköze. Az utóbbi években több olyan sérülékenység jelent meg[31], amelyek az UPnP hibás implementációjából, illetve eredetileg is gyenge biztonsági képességéből, vagy magából a működésből adódnak (például alapértelmezetten a protokollnak nincs hitelesítési funkciója, stb). Javasolt, hogy ilyen szolgáltatás még a hálózaton belül se kerüljön használatra, illetve lehetőleg kerüljön letiltásra mind a kameraeszközökben, mind a határvédelmi vagy router eszközben.

Internet felőli elérés korlátozása

Javasolt, hogy a kamerák és rögzítő eszközök közvetlenül ne legyenek elérhetők az internet felől (például publikus IP cím, port forward, NAT, stb). Amennyiben szükséges elérni az eszközöket távolról, azt csak megfelelő biztonsági garanciák mellett javasolt megtenni. Az interneten publikált eszközök hibás beállításai vagy sérülékenységei távolról kihasználhatók, így kijelenthető, hogy a kockázatok legnagyobb része megszüntethető vagy hatásuk csillapítható, ha az eszközök nem érhetők el közvetlenül az internet felől, hanem csak egy biztonságos VPN kapcsolat kiépülése után válnak hozzáférhetővé.

Biztonságos VPN kapcsolat kialakítása

Az előző pontból kiindulva, ha a kamera csak egy VPN kapcsolaton keresztül elérhető az internet felől, azzal jelentősen lecsökken annak a lehetősége, hogy egy jogosulatlan személy kommunikációt tudjon kezdeményezni az eszközzel. A VPN kapcsolat kiépítése jellemzően nem a kamerák vagy rögzítő eszközök feladata, hanem a különféle routerek vagy határvédelmi tűzfal eszközöké. A VPN hálózaton belüli forgalomszabályozás képes biztosítani, hogy csak azok a felhasználók érhessék el az eszközöket a VPN-en keresztül, akiknek tevékenységéhez erre feltétlenül szükség van.

---

[29] *https://www.securityfocus.com/archive/1/540234*

[30] *https://www.shodan.io/search?query=GoAhead+5ccc069c403ebaf9f0171e9517f40e41*

[31] *Például: https://www.trendmicro.com/en_us/research/19/c/upnp-enabled-connected-devices-in-home-unpatched-known-vulnerabilities.html*

IP korlátozás internet felől

Ha mindenképpen elérhetővé kell tenni az eszközöket az internet felől, és nincs lehetőség VPN kapcsolat kiépítésére, megoldást jelenthet, ha a határvédelmi eszköz csak olyan IP címekről engedélyezi a távoli kapcsolatot, amelyet előre beállítottak a határvédelmi eszközön, például a távoli felügyelet vagy a rendszergazda IP címéről.

IP korlátozás a hálózaton belül

A megfigyelő vagy rögzítő eszközök elérését házon belül is csak olyan felhasználók és rendszerek részére javasolt engedélyezni, akiknek vagy amelyeknek a munkavégzéshez, illetve a működtetéshez feltétlenül el kell érnie ezeket a megoldásokat. A hálózaton belüli elérés-korlátozás kapcsolódik az adatvédelemhez, mert a GDPR alapján az érintettre vonatkozó bármely információ személyes adatnak minősül, pl. az érintett képmása, a róla készült felvétel is. Tehát az adatkezelés megfelelőségéhez biztosítani kell, hogy az élő képhez, illetve a rögzített felvételekhez való hozzáférés dokumentált és szabályozott legyen, azaz meg kell határozni ki férhet hozzá az adatokhoz. Műszaki oldalról a hálózaton belüli IP korlátozás nagymértékben csökkentheti a jogosulatlan hozzáférés, illetve például az esetleges sérülékenységek kihasználásának lehetőségét és kockázatait.

Hozzáférések naplózása és ellenőrzése

A modernebb, a biztonságot szem előtt tartó eszközök naplózzák és rögzítik a hozzáféréseket és a bejelentkezéseket. A biztonsági napló ellenőrzésével észlelhetők a jogosulatlan hozzáférések, ezért vállalati környezetben javasolt a naplózás beállítása és periodikus ellenőrzése. A hosszú távú megőrzés és ellenőrzés érdekében javasolt, hogy a bejelentkezési naplók kerüljenek átirányításra egy központi naplógyűjtőbe, vagy felügyeleti rendszerbe.

Idő- és idő szinkronizáció beállítása (NTP)

A bejelentkezési és hozzáférési időpontok ellenőrizhetősége miatt fontos, hogy a bejelentkezések és hozzáférések ideje pontosan meghatározható és hiteles legyen. Javasolt, hogy az eszközök belső órái kerüljenek beállításra, illetve az eszközök a pontos időt egy belső idő szinkronizációs szervertől automatikusan kérdezzék le.

A hibás bejelentkezések észlelése

Amennyiben az eszköz ezt a funkciót támogatja, javasolt, hogy a hibás, elrontott bejelentkezések észlelésekor automatikus értesítést küldjön, illetve több, elrontott bejelentkezést észlelve az eszköz tiltsa le az érintett hozzáférést (például 5 elrontott bejelentkezési kísérlet után).

Adat és adatfolyam titkosítás

Amennyiben az eszköz támogatja a funkciót, javasolt, hogy a videófolyam továbbítására a Secure RTP (SRTP és SRTCP) protokoll kerüljön alkalmazásra. Az SRTP képes az adatfolyamot titkosítani (AES titkosítás), illetve védelmet nyújt az integritást sértő, illetve a visszajátszás-alapú támadások ellen.

Funkciókhoz való hozzáférés korlátozása

Az eszközök beállításakor figyelmet kell fordítani arra, hogy minden funkció csak és kizárólag a megfelelő hitelesítés után legyen elérhető. Tiltani kell a hitelesítést nem kikényszerítő funkciókat, például a statikus pillanatképek (*snapshot*) elérését, betekintési funkciókat, stb.

Legszűkebb funkcionalitás

A legkevesebb szükséges jogosultság, illetve a legszűkebb funkcionalitás elve szerint javasolt, hogy a nem használt szolgáltatások és funkciók kerüljenek letiltásra. A nem használt szolgáltatásokat (például FTP, SNMP, telnet, SSH, audió/mikrofon szolgáltatás, multicast továbbítás, stb) javasolt kikapcsolni. A rendszer beállításakor javasolt úgy eljárni, hogy az adott felhasználó csak a számára feltétlenül szükséges funkciókat érhesse el az eszközben.

Hálózati monitoring beállítása

A vállalati környezetekben és több megfigyelő kamera alkalmazásakor szükség lehet arra, hogy egy felügyeleti vagy monitoring rendszer ellenőrizze az eszközök megfelelő működését. A legtöbb vállalati eszköz támogatja legalább a *Simple Network Management Protokol* (SNMP) használatát, amelynek beállítása során javasolt az SNMPv1 protokollverzió kerülése, illetve ha az eszköz támogatja, az SNMPv3 (de legalább az SNMv2) alkalmazása. Az SNMPv3 fejlettebb biztonsági funkciókkal rendelkezik és támogatja a hitelesítést, továbbá a monitoring adatforgalom titkosítását.

Adatexport, automatikus adatfeltöltés

Bizonyos eszközök képesek pillanatképeket (*snapshot*), vagy rögzített és helyben (akár rövid időre) eltárolt videófolyamot feltölteni egy külső szerverre. Ha ilyen funkció használatban van, javasolt, hogy a feltöltés csak biztonságos hálózati kapcsolaton és titkosított protokollon (például SFTP) keresztül valósuljon meg. A titkosítatlan kapcsolatok (például FTP) használata általánosan kerülendő, mivel nem tudják garantálni az adatok bizalmasságát és integritását (sértetlenségét).

Üzemeltetés alatt

Sérülékenységi információk követése

Javasolt nyomon követni az üzemeltetett eszközök sérülékenységeit. A legtöbb olyan gyártó, amely értékként kezeli a biztonságot, rendszeresen ad ki tájékoztatásokat az eszközeikkel kapcsolatos sérülékenységekről. A gyártói sérülékenységi listákra, illetve például a *Full Disclosure* [32] listára való feliratkozással értesülhet az üzemeltető az eszközöket érintő sérülékenységekről és megkezdheti a reagálást.

Sérülékenység esetén a firmware frissítése

Ha az üzemeltető a gyártótól, vagy más biztonsági listáról értesül a működtetett eszközök sérülékenységéről, a lehető leghamarabb el kell kezdenie a javítások telepítését. Olyan esetekben, amikor még nem áll rendelkezésre javítás, a gyártók gyakran kompenzációs kontrollok bevezetését javasolják, amelyeket érdemes alkalmazni (ilyen kontroll lehet például a hozzáférések tovább szigorítása).

[32] *https://seclists.org/fulldisclosure/*

Rendszeres firmware frissítés

A sérülékenységektől függetlenül javasolt, hogy az üzemeltető rendszeresen telepítse a gyártó által kiadott új firmware verziókat. Sok esetben ez gondot okozhat, mivel előfordulhat, hogy olyan firmware kerül kiadásra, amelyet nem teszteltek megfelelően, és esetleg problémát okoz az eszköz működésében. Ezt a kockázatot, illetve a frissítési folyamat erőforrásigényét mérlegelve érdemes meghatározni a rendszeres frissítési periódusokat, illetve javasolt lehet a frissítéseket előbb teszt eszközre, vagy csak szűkebb eszközcsoportra telepíteni, és ha nem tapasztalható hiba, szélesebb körben is elvégezni a frissítést.

Rendszeres jelszócserék

A telepítéskor létrehozott felhasználói hozzáférések jelszavainak cseréjét javasolt időnként elvégezni. Ilyen esetekben is mérlegelni kell a folyamatokhoz szükséges erőforrásigényeket és az alapján meghatározni a jelszócsere ütemezését (például évente egy alkalommal).

Felhasználók és hozzáférések rendszeres felülvizsgálata

Az eszközök telepítésekor, illetve beüzemelésekor alkalmazott hozzáférési szabályokat javasolt rendszeresen felülvizsgálni és a már nem szükséges hozzáféréseket megszüntetni. Ha egy felhasználónak már nincs szüksége a hozzáférésre, azt javasolt letiltani vagy törölni. Sok esetben kerülnek beállításra más hálózatokból történő, vagy hálózatok közötti hozzáférések. Ezekre is érvényes, hogy ha már nincs rájuk szükség, akkor a hozzáférő eszköz IP vagy MAC címét ki kell venni az engedélyezési listákból.

Kliens alkalmazások frissítése

A kliens oldali alkalmazások esetében is érdemes nyomon követni az esetleges sérülékenységeket és szükség szerint frissíteni az alkalmazást. Ebben az esetben sem kell megvárni, amíg egy kliens alkalmazással kapcsolatban sérülékenységi információ jelenik meg. Ha a működés ezt lehetővé teszi, törekedni kell a rendszeres frissítésekre.

Hozzáférési naplók rendszeres ellenőrzése

A hozzáférési és audit naplók ellenőrzésével észlelhetők a kamerákhoz, vagy a rögzítő és visszajátszó rendszerhez történő jogosulatlan hozzáférések. Javasolt, hogy az üzemeltetést vagy a felügyeletet ellátó személyek rendszeresen ellenőrizzék a naplózott bejelentkezéseket.

Biztonsági átvilágítás

Javasolt, hogy a kamera hálózatok működését, valamint az eszközök biztonsági funkcióit időnként vizsgálják felül. Az átvilágítás jellemzően a biztonsági és üzemeltetési folyamatokat térképezi fel, értékeli és validálja, illetve olyan eltéréseket keres, amelyek kockázatot jelenthetnek az eszközök és adatok bizalmasságára, sértetlenségére és rendelkezésre állására. A biztonsági átvilágítás kiegészíthető rendszeres (például évi egy alkalommal) sérülékenység vizsgálattal, amely célja, hogy etikus hacker módszerekkel hiányos, vagy nem megfelelő beállításokat, szoftver sérülékenységeket, vagy egyéb biztonsági problémákat keressen és tárjon fel.

Biztonsági javaslatok otthoni eszközök esetén

Az otthoni megfigyelőrendszerek és kameraeszközök esetében hasonló, a legfontosabb pontokban egyező, de kevesebb lépést lehet szükséges megtenni annak érdekében, hogy az eszközök használata ne járhasson a magán- és intimszféra sérülésével.

Beszerzéskor

- alapos, megfontolt kiválasztás
- feltűnően olcsó kamerák kerülése
- az ismeretlen gyártótól származó eszközök kerülése
- a kiválasztott gyártó és eszköz ellenőrzése keresőkben, oldalakon, szakfórumokban
- a kiválasztott kamera biztonsági funkcióinak ellenőrzése

Beüzemeléskor

- dokumentációk, telepítő leírások, biztonsági beállítások alapos tanulmányozása
- az eszköz frissítése a legújabb firmware verzióra
- a gyártó oldaláról letöltött firmware használata
- kliens alkalmazás frissítése a legfrissebb verzióra
- alapértelmezett jelszavak megváltoztatása
- felhasználónév és jelszó beállítása a menedzsment felület eléréséhez
- felhasználónevek és jelszavak létrehozása a kliensekhez, streaming alkalmazásokhoz
- eltérő jelszavak használata
- egyedi, megfelelően erős jelszavak használata
- lehetőség szerint az alapértelmezett felhasználók letiltása
- nem használt, felesleges felhasználók letiltása
- titkosítatlan kommunikáció (pl. HTTP) letiltása
- titkosított kommunikáció (HTTPS, SSL/TLS) engedélyezése, használata
- felhős kapcsolatok ellenőrzése, lehetőség szerint letiltása
- P2P funkció használatának kerülése, lehetőség szerint letiltása
- az UPnP szolgáltatás letiltása az eszközben és a routerben
- a kamera ne legyen elérhető közvetlenül az internet felől
- távoli csatlakozáshoz biztonságos VPN kapcsolat használata
- időbeállítás, idő szinkronizáció beállítása (NTP)
- hozzáférés naplózás beállítása
- biztonságos wifi kapcsolat használata (legalább WPA2-PSK, megfelelő kulcshossz)
- video streaming eléréshez (RTSP) felhasználónév és jelszó beállítása

- statikus *snapshot* elérés letiltása, minden funkció csak hitelesítés után legyen igénybe vehető
- nem használt szolgáltatások tiltása (FTP, SNMP, telnet, SSH, audio, multicast, stb.)
- automatikus állapotkép feltöltése más eszközre csak titkosított (pl. SFTP) kapcsolaton

Üzemeltetés közben

- sérülékenységi információk követése
- sérülékenység esetén a firmware frissítése
- rendszeres (pl. legalább évente) jelszócsere a hozzáférések alatt
- kliens alkalmazások rendszeres frissítése
- hozzáférési naplók rendszeres ellenőrzése

Befejező gondolatok

Előszeretettel alkalmazzák az Internet of Things (IoT) kifejezést minden olyan eszközre, amely kapcsolódik az internethez, illetve adatokat oszt meg más eszközökkel. Egy másik megközelítésben a kutatók és a technológiagyártók inkább intelligens, beágyazott eszközökre alkalmazzák az IoT kifejezést. Használjuk bármelyik értelmezést is, az előrejelzések szerint 2025-re már több mint 40 milliárd olyan eszköz fog kapcsolódni az internethez, amelyet valamilyen szempont alapján IoT címkével látnak el.

Az okosvárosok, a közlekedés, az egészségügy, az ipar és természetesen az okosotthonok eszközei és berendezései potenciális célpontjai a támadóknak, mivel számuk és felhasználhatósági körük robbanásszerű növekedésével egyre inkább megéri ilyen eszközöket támadni és egyre több haszon realizálható az eszközök esetleges sérülékenységeiből, a felhasználók biztonságtudatosságának hiányából, illetve az eszközök helytelen beállításából.

Az IDC előrejelzése[33] szerint az IoT eszközök 2025-re 79,4 zettabájt (ZB) adatforgalmat[34] fognak generálni. A csaknem felfoghatatlan méretű adatmennyiségbe beletartoznak az IoT világhoz tartozó kamerák és megfigyelőeszközök adatforgalmai is, amelyek az IDC becslése szerint a jelzett adatmennyiség jelentős részét fogják kitenni.

Jelen tanulmány arra törekedett, hogy bemutassa az interneten elérhetővé tett, hibás beállítású, illetve esetleges sérülékenységekkel rendelkező hazai felhasználású kamera eszközök használatát, és az ilyen módon alkalmazott eszközök működtetéséből fakadó kockázatokat. A 79 zettabájt adatmennyiségre gondolva tegyük fel a kérdést magunknak, hogy egy ekkora, beláthatatlan adathalmazt tekintve a kamerák által rögzített és korlátozottan vagy korlátozva elérhetővé tett képek és videók vajon mit is jelentenek, illetve fognak jelenteni adat- és információvédelmi szempontból a felhasználók számára?

---

[33] *https://www.idc.com/getdoc.jsp?containerId=prUS45213219*

[34] *1 ZB = 1 000 000 000 000 GB*