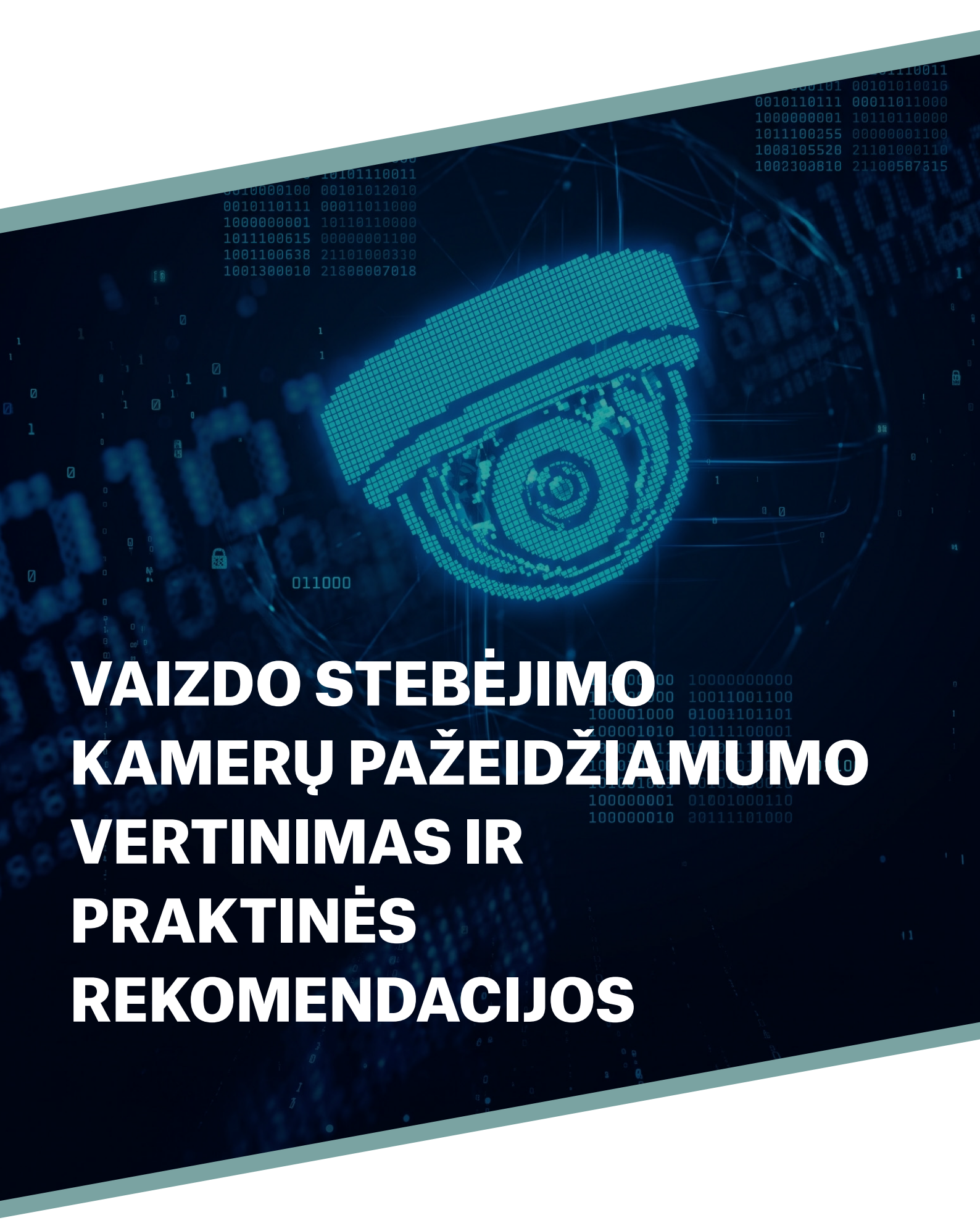


VAIZDO STEBĖJIMO KAMERŲ PAŽEIDŽIAMUMO VERTINIMAS IR PRAKTINĖS REKOMENDACIJOS

ANTRASIS OPERATYVINIŲ TARNYBŲ DEPARTAMENTAS
PRIE KRAŠTO APSAUGOS MINISTERIJOS

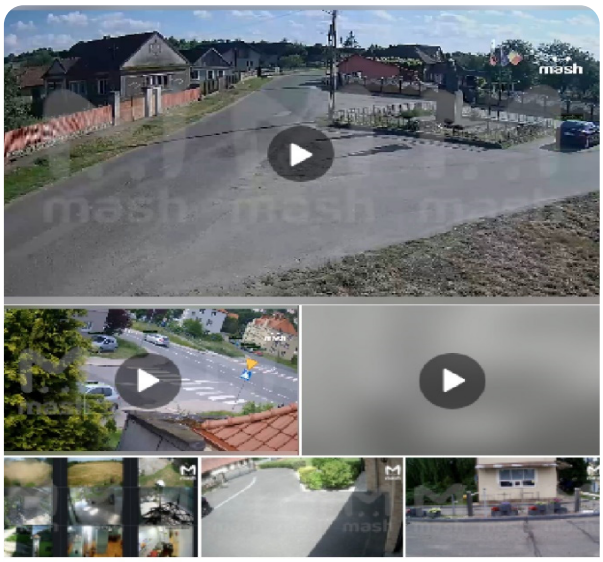
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

VSD LIETUVOS ŽVALGYBA

Vaizdo stebėjimo kameros, užtikrinančios saugumą namuose, įmonėse ir viešose įstaigose, padedančios kontroliuoti gamybos, logistikos ar kitų veiklų efektyvumą, tampa lengvu taikiniu kibernetiniams nusikaltėliams. Jie gali įgyti prieigą prie kamerų ir panaudoti surinktą informaciją nusikalstamai veiklai arba priešiškų valstybių interesams, keliantiems grėsmę nacionaliniam saugumui.

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (NKSC) kartu su Antruoju operatyvinių tarnybų departamentu prie Krašto apsaugos ministerijos (AOTD) bei Valstybės saugumo departamentu (VSD) atkreipia dėmesį, kad net viena neapsaugota kamera gali leisti surinkti reikalingą informaciją arba įsilaužti į visą namų, įmonės ar organizacijos tinklą.

Didžiausią grėsmę kelia galimybė perimti kameros fiksuojamo vaizdo srautą ir taip surinkti jautrią informaciją. Kasdienė veikla energetikos, pramonės, ryšių, vandens tiekimo objektuose ar kariniuose vienetuose, transporto ir žmonių judėjimas, maršrutai, darbo laikas – ši informacija leidžia išanalizuoti, kaip veikia ir kaip yra saugomi įvairūs objektai. Šiuolaikinės vaizdo kameros kaupia ir daug techninės informacijos apie filmavimo laiką, vietą, naudotojų prisijungimus ir gali atpažinti veidus, transporto priemonių valstybinius numerius, fiksuoti vaizdą tamsoje. Tokios informacijos visuma bei stebėjimas ilgesnį laiką leidžia sudaryti išsamų stebimo objekto veiklos modelį, prognozuoti procesus, nustatyti silpnąsias vietas ir pažeidžiamumus.



50 тысяч камер видеонаблюдения в Европе и на Украине взломали российские хакеры — чтобы внедрить в систему ИИ-шпионаж. Теперь наши спецы могут фиксировать все передвижения и объекты, находящиеся внутри стран ЕС и Восточной Европы.

Telegram įrašas apie Europoje ir Ukrainoje perimtas vaizdo stebėjimo kameras

Surinkta informacija panaudojama planuojant kibernetines atakas, sabotažą, pasikėsinimus į asmens gyvybę, fizinių ir juridinių asmenų turtą ar kitokias priešiškas operacijas.

Su Rusija siejami veikėjai užsienio valstybėse jau renka jautrią informaciją, kuri vėliau naudojama karinėms reikmėms. Pavyzdžiui, 2026 m. liepą Nyderlandų žvalgybos tarnybos viešai paskelbė apie nustatytas sistemingas Rusijos skaitmenines šnipinėjimo operacijas išnaudojant vaizdo kameras Vakaruose ir Ukrainoje. Naudodamasi prieigą prie interneto turinčiomis vaizdo kameromis, Rusija perima vaizdo srautą, iš kurio žvalgybos tarnybos vaizdo atpažinimo įrankiais nustato karinių transporto priemonių maršrutus, ginklų pristatymo kelius ir Ukrainos kariuomenės pozicijas.* Pavyzdžiai iš karo Ukrainoje rodo, kad prieigą prie vaizdo stebėjimo kamerų ir su tuo susijusias galimybes Rusijos kibernetiniai įsibrovėliai naudoja karinei informacijai rinkti, įskaitant ir ugnies koregavimui prieš numatytus karinius ir civilinius taikinius, karinę ir svarbią civilinę infrastruktūrą.

Siekdami sumažinti šią riziką, NKSC, AOTD ir VSD rekomenduoja gyventojams bei organizacijoms laikytis kibernetinės higienos principų. Vaizdo stebėjimo sistemos yra svarbi IT infrastruktūros dalis, todėl jų saugumas turi būti užtikrinamas nuolat. Tinkama priežiūra, laiku vykdomi programinės įrangos atnaujinimai ir saugi konfigūracija padeda apsaugoti tiek asmeninę, tiek organizacinę informaciją nuo kibernetinių atakų ir nepageidaujamo šnipinėjimo. Atsakingas požiūris į šių įrenginių saugumą yra būtinas, siekiant užtikrinti saugią ir patikimą aplinką, o kelios minutės, skirtos slaptažodžio pakeitimui ir saugumo atnaujinimų įdiegimui, ne tik apsaugos pačią kamerą, jūsų privatumą, namus ar tinklą, bet ir užtikrins Lietuvos nacionalinį saugumą.

*https://english.aivd.nl/documents/2026/07/10/brochure-cybersecurity-advisory-russian-state-actors-are-compromising-ip-cameras

NKSC, AOTD ir VSD pateikia bazines rekomendacijas dėl vaizdo stebėjimo kamerų, naudojamų namų ūkiuose ir organizacijose:

Pakeisti gamyklinį administratoriaus slaptažodį į naują, stiprų ir unikalų (nesikartojantį per kelis įrangos vienetus) bei nepamiršti jį periodiškai keisti

Reguliariai diegti gamintojo programinės įrangos atnaujinimus, nenaudoti pažeidžiamų saugumo nustatymų (UPnP, SSH, Bonjour, FTP ir Telnet) bei nesaugių protokolų (HTTP ir RTSP)

Įsitikinti, kad nėra apleistų, neprižiūrimų kamerų, nenaudoti gamintojo nebepalaikomų įrenginių ir juos pakeisti naujesne, patikimų gamintojų įranga

Jei nėra būtinybės, neleisti pasiekti kameros tiesiogiai iš interneto, nuotolinei prieigai naudoti tik gamintojo rekomenduojamus sprendimus arba VPN

Išjungti nenaudojamas funkcijas ir paskyras

Įjungti daugiaveiksnį autentifikavimą, jei jis palaikomas (MFA)

Nesirinkti nepatikimų gamintojų vaizdo stebėjimo įrangos, pagamintos Kinijoje, Rusijoje ar Irane. Vengti šių šalių programinės įrangos.

Naudoti tokias funkcijas kaip dalinis vaizdo suliejimas, kai yra tikimybė atskleisti jautrią informaciją (pvz., GPS lokacija)

Riboti vaizdo kameros stebėjimo lauką dėl perteklinių (pvz., išduodančių tikslų adresą) ir konfidencialių (pvz., aukštos rezoliucijos kamerų fiksuojamas vaizdas kompiuterių monitoriuose, dokumentuose ir pan.) detalių fiksavimo;

Stebėti, ar neatsirado jūsų nuosavybėje ar į jūsų nuosavybę nukreiptų jums nepriklausančių vaizdo kamerų