УДК 004.056.53
DOI https://doi.org/10.32838/2663-5941/2021.3/25

Топчій Н.В.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

Білевська О.С.
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

АНАЛІЗ ЗАХИЩЕНОСТІ IP-КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ

Відеоспостереження – основа сучасної системи безпеки. Воно забезпечує безпосередній моніторинг території, допомагає запобігти проникненням зловмисників, виявити підозрілу діяльність, визначити надзвичайні події та провести розслідування. Аналіз відеозаписів може допомогти виявити зловмисників, зокрема спроби підключення до локальної мережі з метою крадіжки важливої інформації.

Технологічний прогрес зробив IP-відеоспостереження одним із найбільш розповсюджених рішень у сфері безпеки. Відеоспостереження все частіше розглядається не тільки як інструмент виявлення, а і як засіб отримання цінної інформації про діяльність співробітників та клієнтів. Відеоспостереження містить багато інформації, тому воно стало джерелом великої загрози.

Можливість використання аналітичних методів для вилучення корисної інформації з відеоданих набуває все більшого значення під час вибору систем відеоспостереження. З одного боку, відеосервери та відеокамери стають усе більш інтелектуальними завдяки нарощуванню процесорних потужностей.

У наш час дуже легко придбати камери відеоспостереження і відеореєстратори, тому що вони мають низьку ціну та повсюдно продаються. Ураховуючи цей споживчий попит, багато виробників розробляють нові IP-камери, WEB-камери і відеореєстратори та не занадто піклуються про деталі їх захисту і вразливості.

Найпоширенішою є практика віддаленого доступу до камер відеоспостереження, адже для реалізації цього не потрібно володіти спеціальним програмним забезпеченням, а можна обійтися просто браузером і простими маніпуляціями, які може провести майже кожна людина. Якщо особа вміє знаходити IP-адреси камер і їх вразливості, то вона може відкрити для себе тисячі камер у всьому світі.

Системи відеоспостереження, які підключені до мережі, дозволяють будувати розподілені системи з можливістю віддаленого доступу та широкими можливостями з інтеграції з іншими системами. Проте їм властиві і проблеми, пов'язані із захищеністю мереж, якими є вразливість даних і пристроїв.

Ключові слова: *IP-камера, відеоспостереження, захист, злам, пароль, підключення, загроза, трафік, комутатор, відеореєстратор.*

Постановка проблеми. Під час установлення камери безпеки або цифрового відеореєстратора необхідно зважати на той факт, що вони схильні до високого ризику зламу програмним забезпеченням, яке автоматично сканує на наявність уразливостей. Отож, важливо знати, як працюють атаки на камери безпеки, щоб захистити системи відеоспостереження. Водночас існує загроза несанкціонованого доступу до ресурсів корпоративної мережі передання даних, яка пов'язана із вадами в налаштуваннях безпеки бездротової мережі.

Аналіз останніх досліджень і публікацій. У серпні 2017 року дослідники з компанії «Checkmarx» провели аналіз захищеності IP-камер Loftek та VStartcam, які найбільш поширені в побуті у всьому світі. Під час дослідження виявлена серія вразливостей, які дозволяють організувати атаки для отримання контролю за пристроями і їх використання для організації комп'ютерних мереж, заражених шкідливим програмним забезпеченням, або для проведення атак на комп'ютери в локальній мережі. Усього під час дослідження камер виявлено 21 вразливість, які можна зарахувати до категорії безпечних, або помірних. Серед наявних проблем виокремлюються зумовлені параметри входу без повідомлення про необхідність зміни пароля за замовчуванням, відсутність підтримки HTTPS (Hyper Text Transfer Protocol Secure), а також проблеми CSRF (Cross-site Request Forgery), які дозволяють використовувати iFrame (Inline Frame) для відправки команд на камери, що містяться у внутрішній мережі користувача, який зайшов на сторінку. Для приховування своєї присутності після успішного

отримання контролю над пристроєм зловмисник може завести нового користувача з ім'ям «%20» і порожнім паролем, який не буде помітний у списку користувачів в інтерфейсі адміністратора.

Експерт компанії Positive Technologies Ілля Сміт виявив і допоміг усунути критичну вразливість у вбудованому програмному забезпеченні IP-камер компанії Dahua, які широко використовуються для відеоспостереження в банківському секторі, енергетиці, телекомунікації, транспорті, системах «розумний дім» та інших сферах. Ця вразливість отримала назву «CVE-2017-3223» та є пов'язаною з можливістю переповнення буфера у web-інтерфейсі Sonia, який призначений для дистанційного керування і налаштуваннями камер. Неавторизований користувач може відправити спеціально сформований POST-запит на вразливий web-інтерфейс і віддалено отримати привілеї адміністратора, що надає необмежений контроль над IP-камерою.

Незважаючи на значну кількість наукових публікацій, присвячених проблемам захищеності IP-камер, стрімкий розвиток систем комунікації та протоколів їх захисту зумовлює потребу подальших досліджень цієї тематики.

Постановка завдання. Метою статті є аналіз захищеності IP-камер відеоспостереження, виявлення нелегітимної активності з можливістю блокування несанкціонованих підключень до пристроїв або оповіщення сторонніх засобів фільтрації і блокування трафіка. Метою аналізу є своєчасне виявлення потенційних загроз і реагування на них (без негативного впливу на функціонування мережі відеоспостереження).

Виклад основного матеріалу дослідження. Для застосування найбільш ефективних інструментів захисту необхідно виокремити види загроз та провести аналіз методів нападу на системи відеонагляду. Можна виокремити три основних типи загроз для систем відеоспостереження:

- злам для отримання доступу до даних;
- злам для перехоплення керування або відключення системи;
- злам із метою несанкціонованого використання обчислювальних потужностей системи.

На стадії аналізу вразливостей системи необхідно врахувати, що системи відеоспостереження можуть використовуватися, зокрема, для розв'язання технологічних завдань і організації бізнес-процесів підприємства. Тому можливою ціллю зловмисників може бути інша система, а обладнання системи відеоспостереження може використовуватися як проміжний етап атаки. Крім того, система відеоспостереження, як правило, інтегрована з іншими підсистемами безпеки і системами автоматизації. Питання інформаційної захищеності системи відеоспостереження переходить у завдання захисту всіх систем, у які вона інтегрована або з якими обмінюється даними.

В аналогових системах відеоспостереження відеокамера відправляє відеосигнал на монітор безпосередньо без стиснення. Це прості в монтажі, надійні, але громіздкі системи з обмеженим функціоналом. Сьогодні такі рішення використовують лише в невеликих системах із декількома камерами, які розміщені близько одна до одної або у вузькоспеціалізованих галузях. Аналогові системи мають обмежений функціонал і можуть тільки вести спостереження в режимі реального часу, а також записувати відеоінформацію на цифрові накопичувачі (DVR – Digital Video Recorder). Розширення функціоналу потребує витрат на додаткові пристрої і їх монтаж. Запис на DVR також має обмеження: декодування відео відбувається безпосередньо в DVR, а не на відеокамерах. Так, пристрій DVR необхідно фізично з'єднати з кожною камерою за допомогою кабелю.

IP-камера відеоспостереження знімає відео і транслює відеопотік у цифровому форматі з використанням мережевого протоколу, який забезпечує маршрутизацію пакетів. Тобто IP-камера складається з матриці, об'єктива, центрального процесора, процесора обробки, процесора стиснення та мережевого інтерфейсу. IP-камери відеоспостереження є самодостатнім окремим засобом спостереження, керування якими здійснюється через WEB-інтерфейси, передаючи всі потоки мережі. Майже всі сучасні цифрові IP-камери відеоспостереження побудовані на операційній системі Linux, яка дуже обмежена і має тільки найбільш необхідне для роботи. Сама по собі операційна система Linux безкоштовна, дуже надійна і стійка до зовнішніх впливів і зламів, тому виробники і будують на її базі відеореєстратори, відеосервери, камери відеоспостереження та інші пристрої.

Наявність модуля Wi-Fi і мережевого інтерфейсу RJ-45 дозволяють проводити безпосереднє підключення до IP-камер. Раніше для цього використовувалися спеціальні додатки, але зараз все можна проводити через стандартний браузер із мобільного телефона або комп'ютера. Їх слабкість у тому, що вони завжди включені і мають віддалений доступ, чим активно і користуються зловмисники.

Перевагою сучасних IP-камер є великий «інтелект», як-от система увімкнення запису за

розпізнаванням руху, автоматичне відстеження руху, виявлення залишених предметів, цифровий зум і фотофіксація особи, номера машини тощо. Крім того, IP-камери можуть стискати відео, відправляючи картинку з безлічі камер через один кабель. За допомогою кодування можна стискати відеофайли, скорочуючи завантаженість лінії зв'язку до 80%. Це зменшує вимоги до обсягів мережевих накопичувачів (NVR – Network video recorder), які можуть зберігати відеозаписи з якістю 720p тривалістю до 50 днів на жорсткому диску обсягом 4 Тб.

Зв'язок із NVR може здійснюватися через мережу Інтернет, тобто на основі IP-камер можна побудувати розподілену систему відеоспостереження, яка буде передавати дані відеозапису через мережу на віддалений накопичувач. Таку систему можна контролювати віддалено, зокрема з мобільних пристроїв, а мережевий накопичувач фізично не є доступним для потенційних зловмисників, оскільки може перебувати за сотні кілометрів від контрольованого об'єкта. Проте будь-які проблеми з переданням інформації можуть призвести до повного або часткового порушення працездатності системи.

Слід зазначити, що більшість IP-камер мають функцію P2P (Peer-to-peer) і можуть працювати без статичної IP-адреси, поєднуючи камеру і монітор через інтернет-сервер виробника камери. Мережа з функцією P2P заснована на рівноправності учасників. Найчастіше в такій мережі відсутні виділені сервери, а кожен вузол є як клієнтом, так і виконує функції сервера. Така організація дозволяє зберігати працездатність мережі за будь-якої кількості і будь-якому поєднанні доступних вузлів. Ця функція дозволяє організувати відеоспостереження у тому разі, коли провайдер не надає статичні IP-адреси. Крім того, налаштування камер P2P дуже просте.

Коли відбувається підключення камери з функцією P2P, їй присвоюється номер. За його допомогою відбувається визначення сервером можливості передання даних на сервері. Ідентифікатор звіряється і користувач отримує доступ до відеопотоку через персональний комп'ютер або пристрій під керуванням Android чи iOS. Крім отримання інформації, можна здійснювати безпосереднє керування роботою камери.

З одного боку, функція P2P в IP-камерах надає багато переваг, проте ця функція здатна змінити конфігурацію DMZ (Demilitarized Zone) на маршрутизаторі. DMZ – це спеціалізований локальний сегмент мережі, який містить загальнодоступні сервіси з повним відкритим доступом для внутрішньої та зовнішньої мережі. У налаштуваннях маршрутизатора не можна використовувати для системи відеоспостереження функцію DMZ, оскільки вона може надати зловмисникові необмежений доступ до відеокамери, яка перебуває в мережі.

Для захисту лінії дротового зв'язку потрібно використовувати керовані комутатори. Необхідно здійснювати фільтрацію за MAC-адресою з підтримкою «білих» списків, роботу з VLAN, VPN, блокування портів, які не використовуються. Деякі комутатори можуть самі шифрувати вхідні дані та передавати їх далі на пристрій, який буде розшифровувати вхідний потік. Також комутатори можуть відслідковувати спроби недозволеного доступу або будь-які зміни в локальній мережі і повідомляти про них адміністратора системи.

Бездротові Wi-Fi IP/P2P-камери можуть заощадити значні засоби на встановленні відеоспостереження. Наразі пропускної здатності Wi-Fi мережі достатньо для передання відео високої роздільної здатності. Проте канал Wi-Fi може бути блокований DDoS-атаками, відправленими через радіоканал, які спрямовані на порушення якості функціонування мережі або на абсолютне припинення доступу користувачів.

У цьому разі перерветься потік відео, який іде від камери на мережевий відеореєстратор. При цьому відключення мережі не означає припинення відеоспостереження, адже сучасні відеокамери мають убудовані карти пам'яті, які дозволяють згодом «вручну» переглянути відеозапис.

Загрозою конфіденційності відеоспостереження через мережу Wi-Fi є радіосніферінг. Сніфери займаються перехопленням та аналізом мережевого трафіка. Для того, щоб підвищити стійкість Wi-Fi мережі відеоспостереження, провести захист периметра і виявити спроби підключення небажаних користувачів, застосовуються програмно-апаратні комплекси. Ці прилади безперервно сканують кожен канал Wi-Fi і автоматично виявляють різнотипні загрози, включаючи поширені атаки шляхом перебору паролів, уторгнення за допомогою утиліт Airpwn, фазинг тощо. Програмне забезпечення сповіщає оператора про спробу вторгнення і дозволяє виявляти джерела перешкод, «глушилки» сигналу й іншу підозрілу активність у всьому діапазоні частот Wi-Fi, а також у мережах мобільного зв'язку 3G, 4G LTE і CDMA.

Необхідно враховувати безпеку не тільки камер, а і всієї інфраструктури, оскільки зловмисникам досить одного слабкого місця, щоб отримати доступ до всієї системі. Захищений зв'язок між камерами і мережевими компонентами забезпечується

шляхом призначення кожному елементу ключа автентифікації. Це електронний підпис, необхідний для перевірки всіх компонентів (від камер до керівного програмного забезпечення). Для забезпечення безпеки всього процесу автентифікації пристрої повинні підтримувати автентифікацію на основі імені користувача і пароля (IEEE 802.1x).

Для захисту даних відеоспостереження першочергове значення має шифрування потоків даних і збереженої інформації. Ефективний варіант реалізації шифрування на апаратному рівні – це використання у всіх IP-камерах і записувальних пристроях довіреного модуля TPM (Trusted Platform Module). Цей модуль є надійним сховищем криптографічних ключів для захисту даних. У разі зламу пристрою зловмисники не зможуть скористатися витягнутою з нього інформацією. Коли дані потрапляють у керівне або клієнтське програмне забезпечення, криптографічний ключ допомагає розшифрувати дані, а також підтверджує, що камера – аутентифікований мережевий партнер.

Ступінь конфіденційності даних відеоспостереження може варіюватися від несекретної до цілковито секретної. Але навіть мережі з надійними пристроями і безпечними каналами передання даних можуть стати жертвами людської помилки, тому надійні відеосистеми пропонують варіанти керування особистими правами доступу користувачів і підтримують дійсні галузеві стандарти. Рішення для інформаційного захисту систем відеоспостереження повинні відповідати провідним галузевим стандартам інфраструктури відкритих ключів PKI (Public Key Infrastructure). Можливі варіанти використання власних PKI-рішень виробника з власним сертифікаційним центром або підтримка сторонніх PKI-рішень.

Зміна пароля за замовчуванням для цифрового відеореєстратора або IP-камери не гарантує абсолютного захисту пристрою від атак зловмисників. Технічні фахівці під час установлення IP-камери або цифрового відеореєстратора змінюють пароль, установлений за замовчуванням, на інший, який видається більш безпечним і гарантує, що зловмисник не зможе проникнути в систему. Ця процедура може допомогти, але не вирішує проблему захисту загалом. Камери відеоспостереження мають внутрішню операційну систему, а також інші програми, які можуть мати вразливості та дають можливість використовувати їх для отримання доступу до системи.

Висновки. Таким чином, можна виокремити основні рекомендації із гарантування безпеки бездротових Wi-Fi мереж:

Швидкий розвиток IP-відеоспостереження й інших мережевих систем безпеки вимагає безперервної співпраці між інтеграторами та виробниками для створення і реалізації передових методів, необхідних для забезпечення кібербезпеки.

Розглянемо основні способи рекомендації із гарантування безпеки, які пов'язані із системами відеоспостереження. Використовуючи їх, можна побудувати комплексну ефективну програму профілактики і реагування.

По-перше, необхідно регулярно проводити перевірку вразливості всіх компонентів системи IP-відеоспостереження. Ця перевірки повинна включати тестування всіх протоколів, апаратних засобів та прошивки. Таким чином, кожен компонент системи відеоспостереження буде ретельно перевірений на здатність протистояти кібератакам. Тестування протоколу – це перевірка безпеки мережевих комунікацій, надійності шифрування і можливості несанкціонованого перехоплення даних. Аналіз прошивки пристроїв повинен обов'язково містити встановлення доступних оновлень.

По-друге, необхідно обмежити кількість користувачів та мінімізувати фізичний доступ до системи IP-відеоспостереження. Чим більше людей можуть впливати на роботу компонентів або даних системи, тим більша ймовірність того, що система залишиться відкритою для кібератак.

По-третє, не можна використовувати паролі за замовчуванням. Підібрати до системи пароль (якщо він був установлений виробником) – не досить складно. Обов'язково необхідно міняти паролі до обладнання, які встановлені за замовчуванням. Таким чином, є велика ймовірність уникнення найбільш поширеної помилки жертв хакерських атак.

Не зайвим буде розглянути і заходи фізичної захисту систем відеоспостереження.

– використання замикальних телекомунікаційних шаф;

– розміщення серверного і важливого комутаційного обладнання у виокремленому замикальному приміщенні;

– прокладання кабелів у важкодоступних місцях;

– використання для прокладення і монтажу кабелів труб, закритих лотків і боксів, монтажних коробок;

– використання обладнання в спеціальному антивандальному виконанні на особливо відповідальних ділянках або в легкодоступних місцях.

Список літератури:

1. Дудатьев А.В., Баришев Ю.В., Войтович О.П. Метод оцінювання безпеки інформаційних ресурсів підприємства на основі аналізу вразливостей. *Вісник Хмельницького національного університету*. № 4. 2008. С. 78–83.
2. Erez Yalon, Exposing Wireless IP Camera Security Flaws. URL: www.checkmarx.com.
3. Орлов С. IP-камеры с интеллектом. *Журнал сетевых решений/LAN.* 2013. № 11. С. 44–63.
4. Полевщиков А.А. *Кибербезопасность сетевого видеонаблюдения: теория и практика. Алгоритм безопасности.* 2017. № 5. С. 30–32

Topchii N.V., Bilevska O.S. ANALYSIS OF THE SECURITY OF IP SURVEILLANCE CAMERAS

Video surveillance is the basis of a modern security system. It provides direct monitoring of the territory, helps prevent intruders from entering, detect suspicious activity, detect emergencies and conduct investigations.

Video analysis can help detect intruders, including detecting attempts to connect to a local network in order to steal important information.

Technological advances have made IP video surveillance one of the most common security solutions. Video surveillance is increasingly seen not only as a detection tool, but also as a means of obtaining valuable information about the activities of employees and customers. Video surveillance contains a lot of information, so it has become a source of great threat.

The ability to use analytical methods to extract useful information from video data is becoming increasingly important when choosing video surveillance systems. On the one hand, video servers and camcorders are becoming more intelligent thanks to the increase in processing power.

Nowadays, it is very easy to buy CCTV cameras and DVRs because they have a low price and are sold everywhere. Taking into account this consumer demand, many manufacturers are developing new IP cameras, WEB cameras and video recorders, but they do not care much about the details of their protection and vulnerabilities.

The best practice of remotely accessing CCTV cameras is due to their poor security. To implement this, you do not need to have special software, you can do just a browser and simple manipulations that can be carried out by almost everyone. If a person knows how to find the IP addresses of cameras and their vulnerabilities, then he can discover thousands of cameras around the world.

Video surveillance systems that are connected to the network allow you to build distributed systems with the ability to remotely access and ample opportunities for integration with other systems. However, they also have problems that are associated with the security of networks – first of all, the vulnerability of data and devices.

Key words: *IP camera, video surveillance, protection, hacking, password, connection, threat, traffic, switch, video recorder.*