УДК 004.056

Ян Володимирович ХАШЕВ,
студент 2 курсу магістратури факультету № 6
Харківського національного університету внутрішніх справ

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ З КОМП'ЮТЕРНИХ МЕРЕЖ ВІДЕОСПОСТЕРЕЖЕННЯ

Приймаючи до уваги стрімкий розвиток інформаційний технологій, а також для більшого розуміння важливості якісної організації безпеки систем відеоспостереження (Video Surveillance Systems, VSS), важливо відмітити, що на сьогоднішній день це не просто відеосистеми, а повноцінні інтернет-речі (Internet of things, IoT), яких офіційно, за статистичними даними станом на 2014 рік, встановлених професійними компаніями, у всьому світі функціонувало 245 мільйонів камер спостереження [1]. Сучасні засоби відеоспостереження здатні зберігати, оброблювати інформацію, «комунікувати» між собою та впливати на прийняття рішень, тому ці системи повинні відповідати вимогам інформаційної безпеки.

Як правило, більшість проблем, пов'язаних із системами відеоспостереження, стосуються питання конфіденційності, однак є й інші, не менш важливі. Наприклад, небезпечна або скомпрометована мережева система відеоспостереження може створювати ризики викрадення для установ, що працюють з грошовими коштами (банківські установи, підприємства), створюють емоційний вплив на інших осіб (особливо дітей) або втручаються у діяльність правоохоронних органів.

У 2016 році, в результаті дії хробака та ботнета «Mirai», використовуючи банальні вразливості у вигляді однакового, незмінного, встановленого виробником пароля доступу до облікового запису адміністратора на пристрої типу інтернет-речі (IoT), окрім побутових приладів, було уражено та скомпрометовано більш ніж 100 тисяч камер відеоспостереження та відеореєстраторів, тобто прилади, призначені для забезпечення безпеки, стали самі представляти загрозу. Наслідком цього було використання скомпрометованих камер та інших інтернет-речей для здійснення масових DDoS-атак на великі компанії [2].

Дійсна стаття присвячена висвітленню основних проблем, що стосуються організації захисту даних під час експлуатації мережевих систем відеоспостереження, та практичним рекомендаціям для забезпечення відповідної інформаційної безпеки..

Досліджуючи питання безпеки та захисту інформації від витоку з комп'ютерних мереж систем відеоспостереження, аналізуючи публічно виявлені вразливості та опубліковані експлойти, пов'язані із VSS, пропонується наступна класифікація критеріїв для опису загроз, вразливостей, атак та їх наслідків для систем відеоспостереження:

1) об'єкт (поверхня) атаки; 2) вид атаки; 3) спосіб з'єднання під час атаки; 4) компонент, який безпосередньо зазнав нападу; 5) складність експлуатації; 6) наслідки; 7) складність відновлення наслідків атаки [3].

Об'єктом (поверхнею) атаки на мережеві системи відеоспостереження можуть виступати: веб-інтерфейс або функція механічних панорамних поворотів (Pan-Tilt-Zoom, PTZ); оновлення програмного забезпечення; налагоджувальний порт (Debug Port) або USB-порт; візуальний рівень, що використовує семантику і розпізнавання зображень; шкідливі зображення та стенографія; використання оптичних прихованих каналів передачі даних (VisiSploit); радіо або WiFi канали.

Видами атаки можуть бути наступні: використання слабкого парольного доступу до мережевих відеосистем; недостатній захист транспортного рівня; DoS-атака; міжсайтовий скриптинг (XSS); міжсайтова підробка запиту (CSRF); підміна шляху до файлу (Path traversal); переповнення буферу; реверс інжиніринг; здійснення оновлень через невідомі джерела; несанкціонована передача конфіденційних даних до місця, що контролюється елементом загрози (Data exfiltration); прослуховування радіомережі та каналу WiFi, створення перешкод; інше.

З'єднання під час атаки на VSS може бути фізичне (локальне) або мережеве (віддалений або локальний доступ).

Ураховуючи, що системи відеоспостереження можуть використовуватись також для вирішення технологічних задач та організації бізнес-процесів, потенційною метою зловмисників може бути інша система, а компрометація обладнання системи відеоспостереження виступатиме лише як проміжний етап атаки. Окрім того, системи відеоспостереження, як правило, інтегруються із іншими підсистемами безпеки, тому питання захисту інформації переходить в задачу захисту інформаційної безпеки всіх систем.

Для забезпечення інформаційної безпеки систем відеоспостереження, перш за все, необхідно використовувати комплексний підхід, який включає всю інфраструктуру, що складається з камер, серверного обладнання, клієнтських робочих місць, приладів збереження даних, мережевих протоколів та інфраструктури керування ключами. А. О. Полевщиков, менеджер компанії Bosch, виділяє чотири важливих етапи побудови безпечної системи відеоспостереження [4]:

1. Створення довіреної інфраструктури. Захисний зв'язок між камерами та мережевими компонентами забезпечується шляхом надання кожному елементу системи ключа аутентифікації (електронного підпису) на основі ім'я користувача та паролю (IEEE 802.1x), а також використання EAP-TLS, що забезпечує безпеку всього процесу аутентифікації.

2. Захист даних. Шифрування потоку даних та збереження інформації є головною метою захисту даних систем відеоспостереження. Ефективним варіантом шифрування на апаратному рівні є використання довіреного платформного модулю (TPM).

3. Керування правами доступу користувача.

4. Відповідність галузевим стандартам. Рішення для інформаційної безпеки систем відеоспостереження повинні відповідати стандартам інфраструктури відкритих ключів (PKI).

Для об'єктів життєзабезпечення діяльності підприємства з питань інформаційної безпеки в загальному вигляді рекомендовано дотримуватись стандартів з захисту інформації, а саме міжнародний стандарт в галузі IT ISO/IEC 27001 («Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги»), а серед конкретних, практичних заходів окремо зазначимо наступні [4]:

– обмеження кількості доступних IP-адрес, що не використовуються, за допомогою служби IPAM (IP Address Management, Управління IP-адресами), що дозволяє зменшити можливість зовнішніх кібератак на систему, які здійснюються несанкціонованими, локально підключеними мережевим пристроями;

– обмеження доступу до мережі через безпеку портів на граничних комутаторах, наприклад, лише конкретна MAC-адреса може отримати доступ до конкретного порту;

– створення політики паролів та дотримання загальноприйнятих вимог щодо парольного доступу, а саме: кількість символів не менш восьми; повинен містити букви верхнього та нижнього регістру, спеціальний символ та цифри. Паролі повинні оновлюватись з плином часу на основі затвердженого регламенту;

– виключення або деактивація портів та протоколів, які допускають більш низький рівень доступу, а також тих, що не використовуються;

– виключення та перенаправлення портів HTTP або HTTPS;

– деактивація підтримки мережевого протоколу Telnet (порт 23/TCP) на всіх пристроях до моменту, коли протокол не знадобиться для ремонту або усунення несправностей;

– виключення або тунелювання з використанням HTTPS-протоколу сервісу потокової передачі відео в реальному часі (RTSP) для уникнення буферних атак за допомогою переповнення стеку;

– уникнення використання набору мережевих протоколів UPnP (Universal Plug and Play) у великих системах;

– під час налаштування IP-відеопристрою для багатоадресного використання необхідно змінити TTL-пакет на значення, яке дорівнює максимальній кількості переходів (якщо відомо) або виставити його 15;

– використання VPN або VLAN, за допомогою яких підвищується загальний рівень безпеки;

– налаштування IP-відеопристроїв як клієнтів на основі стандарту IEEE 802.1x спільно з EAP-TLS для забезпечення безпечного зв'язку.

Таким чином можна зробити висновок про те, що поширення систем відеоспостереження, незважаючи на їх призначення забезпечити безпеку людей, є істотним джерелом загроз та ризиків втрати конфіденційних даних як для підприємств, установ та організацій, так і для фізичних осіб, тому питання організації захисту даних під час встановлення та експлуатації мережевих систем відеоспостереження є дуже важливим, а дотримання міжнародних стандартів з інформаційної безпеки, загальноприйнятих правил та використання вище наведених практичних рекомендацій для досягнення зазначеної мети – обов'язковим.

Список бібліографічних посилань

1. Jenkins N. 245 million video surveillance cameras installed globally in 2014. June 2015 // Market Insight / HIS Market. URL: https://technology.ihs.com/532501/245-million-video-surveillance-cameras-installed-globally-in-2014 (дата звернення: 28.10.2018)..

2. Ляпін Д. Кібербезпека для систем відеоспостереження: загрози та ризики. // RUБЕЖ: інформаційно-аналітичний журнал. URL: www.ru-bezh.ru/svoimi-slovami/19192-kiberbezopasnost-dlya-sistem-videonablyudeniya-ugrozyi-i-riski (дата звернення: 28.10.2018)..

3. Costin Andrei. Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations. // Conference: 6th International Workshop on Trustworthy Embedded Devices (TrustED 2016), Vienna, Austria, October 2016. / ResearchGate. URL: www.researchgate.net/publication/307866768_Security_of_CCTV_and_Video_Surveillance_Systems_Threats_Vulnerabilities_Attacks_and_Mitigations#pf7 (дата звернення: 28.10.2018)..

4. Полевщиков А. О. Кібербезека мережевого відеоспостереження: теорія та практика. *Журнал «Алгоритм безпеки»*. 2017. № 5. URL: https://algoritm.org/arch/17_5/17_5_14.pdf (дата звернення: 28.10.2018).

Одержано 28.10.2018