кодування дозволяє базі даних розрізняти код і дані, незалежно від того, що саме ввів користувач.

Підготовлені інструкції гарантують, що зловмисник не зможе змінити призначення запиту, навіть якщо команди SQL вставлені зловмисником. У безпечному прикладі, якщо зловмисник повинен був ввести ідентифікатор користувача *tom' or '1'= '1*, параметризований запит не був би вразливий і замість цього шукав би ім'я користувача, яке буквально відповідало всій рядку *tom' or '1'= '1*.

Розробникам подобається підхід, заснований на підготовлених операторах, оскільки весь SQL-код залишається в додатку. Це робить додаток відносно незалежним від бази даних.

Список бібліографічних посилань

1. Gregg Keizer (April 25, 2008). "Huge Web hack attack infects 500,000 pages". Archived from the original on October 19, 2015. Retrieved October 16, 2015.

2. Stephen W., Keromytis D. (2010), SQLrand: Preventing SQL Injection Attacks, Department of Computer Science Columbia University.

3. Michael Zino (May 1, 2008). "ASCII Encoded/Binary String Automated SQL Injection Attack". Archived from the original on June 1, 2008.

4. Justin C. "Using SQLBrute to brute force data from a blind SQL injection point". Archived from the original on June 14, 2008. Retrieved October 18, 2008.

5. Ronald L. (2008), "SQL Injection", Hong Kong Computer Emergency Response Team Coordination Centre.

Одержано 31.10.2018

УДК 004.056

Тетяна Петрівна КОЛІСНИК,
кандидат педагогічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0002-7442-8136;
Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-4794-743X

ОСОБЛИВІ ПИТАННЯ ЗАХИСТУ СИСТЕМ IP-ВІДЕОСПОСТЕРЕЖЕННЯ

На теперішній час як у системі Міністерства внутрішніх справ так і на державному та регіональних рівнях впроваджуються різні програми та заходи безпеки. Так, наприклад у березні 2018 року на сесії Харківської обласної ради була прийнята «Програма забезпечення публічної безпеки і порядку та протидії злочинності на території Харківської області на 2018-2019 роки», відповідно до якої

будуть придбатися системи відеоспостереження, стаціонарні переговорні пристрої для термінового виклику спецслужб, електронні планшети, відеореєстратори, відеотехніка та сучасні засоби зв'язку для груп швидкого реагування та правоохоронців.

Серед завдань програми є:

– удосконалення науково-методичного, матеріально-технічного та інформаційного забезпечення правоохоронних та інших органів, що беруть участь у забезпеченні публічної безпеки та порядку;

– безперервний моніторинг криміногенної ситуації в області, в т.ч. за рахунок соціологічних технологій та забезпечення своєчасного реагування на негативні зміни;

– здійснення посиленого контролю за ситуацією у публічних місцях, передусім при проведення заходів за участю значної кількості громадян;

– запобігання правопорушенням, що вчиняються з використанням телекомунікаційних мереж та мережі Інтернет [1, с. 216].

У системі Міністерства внутрішніх справ впроваджено низку аналітичних систем з можливістю проведення глибокого аналізу великих масивів інформації, включаючи відкриті джерела де на першому рівні є система відеомоніторингу, наприклад, єдиний аналітичний сервісний центр (UASC) поліції, створений за прикладом системи безпеки Абу-Дабі при ГУНП в Донецькій області.

Системи відеоспостереження – це програмно-апаратний комплекс (відеокамери, об'єктиви, монітори, реєстратори та ін. устаткування), призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах. Відеоспостереження є сьогодні невід'ємним елементом будь-якої сучасної системи публічної безпеки та порядку [1, с. 217].

В умовах створення різних сучасних систем безпеки, у тому числі систем публічної та кібербезпеки конкурентоздатну альтернативу складають системи мережевого або IP-відеоспостереження, основою для яких є IP-камери. Такі системи не вимагають прокладення додаткових ліній зв'язку, передача даних відбувається по мережевій інфраструктурі, побудованій на протоколі IP.

Контроль та адміністрування системи здійснюється з будь-якого комп'ютера, що має доступ до мережі та спеціальне програмне забезпечення.

Зараз IP-камери за ціною набагато перевищують вартість аналогових камер, але зберігаючи такий темп розвитку виробництва, незабаром вони стануть доступнішими.

При створенні технічного завдання для проектування оптимальної системи відеоспостереження слід розглянути типові технології побудови таких систем, їх переваги та недоліки. Так, при використанні аналогових систем відеоспостереження відомі виробники, наприклад компанія BOSH пропонує спеціальний модуль для конвертації «аналогової» камери в IP-пристрій [1, с. 218].

Ключовим елементом мережі IP-відеоспостереження є мережева IP-відеокамера яка має об'єктив, оптичний фільтр, ПЗС-матрицю (прилад із зарядним зв'язком), вбудований мікропроцесор для оцифровування/стискування відеозображення, мережевий контролер для підключення в мережу Ethernet та інші елементи. Найголовніше, що кожна мережева відеокамера має свій власний IP-адрес, обчислювальні функції та вбудоване ПЗ, що дозволяє їй функціонувати як повноцінний мережевий пристрій.

На відміну від аналогової відеокамери, IP-камера не потребує прямого підключення до комп'ютера або до будь-яких інших апаратних або програмних засобів. Її підключення може здійснюватися як за допомогою дротяного з'єднання (по міді або оптичному волокну), так і безпровідного (Wi-Fi, GPRS/EDGE, 3G, супутниковому зв'язку та ін.). Таким чином, досягається повна або часткова мобільність користувача, який здатний стежити за видаленими об'єктами практично з будь-якої точки земної кулі.

Тому слід виділити наступні переваги таких систем IP – відеоспостереження, а саме:

1. Оператор системи може здійснювати візуальний контроль як локально, так і віддалено (з ПК, мобільного телефону і так далі), здійснювати функції адміністрування системи відеоспостереження використовуючи переваги веб-технологій.

2. Спрощеність та малі витрати на встановлення й монтаж. Мережеві відеосистеми IP не вимагають прокладення додаткового коаксіального кабелю, як в аналогових системах, а підключаються до існуючої локальної мережі відеоспостереження за об'єктом за допомогою безпровідних технологій.

3. Якість відеозображення. В сучасних IP-системах застосовується формат MPEG-4, який дозволяє ефективніше використовувати ресурси мережі в порівнянні з форматом M-JPEG.

4. Можливість передавати по одній лінії зв’язку не лише відеосигнал, але й звук, а також управляти та адмініструвати IP-камери.

5. Гнучкість й масштабованість систем IP- відеоспостереження полягає в можливості будівництва фізично розподілених мереж відеомоніторингу, контролю і дистанційного керування без прив'язки до відстані.

6. Інтеграція з багатьма існуючими на даний момент системами відеоспостереження.

Критеріями вибору на користь IP – камер при проектуванні таких систем на теперішній час також є:

– наявність каналу зв’язку з високого пропускною спроможністю від 100 Мб/с і вище та вільних портів Ethernet;

– за рахунок вбудованих в камери WEB серверів при рішенні завдань видаленого моніторингу контрольованого об'єкту (без використання архівної інформації) з використання мережі Інтернет;

– завдання вимагають високого розділення, при невисоких вимогах до освітленості, розміру кадру і ін. (З дозволом більш 1 Мпиксель) [1, с. 219].

Виходячи з проведеного аналізу існуючих на ринку готових систем відеоспостереження, найбільш перспективними технологіями відео-спостереження є IP-відеоспостереження, яке легко розгортається та базується на сучасних комп'ютерних мережах стандарту Ethernet.

Нормальне функціонування систем IP-відеоспостереження та її складових таких як мережеві екрани, брандмауери, фаєрволи, системи резервного копіювання, антивірусні засоби та інші) неможливо без стандартних засобів захисту, тому існує необхідність використання IDS (СВВ – систем виявлення вторгнень), які є основним засобом боротьби з мережними атаками [2].

Системи виявлення вторгнень починають усе ширше впроваджуватися в практику забезпечення безпеки корпоративних мереж які у свою чергу можуть використовувати системи IP-відеоспостереження.

Системи виявлення вторгнень забезпечують виявлення:

– мережевих атак проти вразливих сервісів;

– атаки спрямовані на підвищення прав користувачів;

– неавторизований доступ до важливих файлів;

– дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

Використання СВВ допомагає досягнути такі цілі:

– виявити вторгнення або мережеві атаки;

– забезпечити належний контроль якості адміністрування, особливо у великих і складних мережах;

– спрогнозувати можливі майбутні атаки і виявити вразливості для запобігання їх подальшого розвитку;

– отримати корисну інформацію про проникнення, для відновлення і налаштування конфігурації мережі;

– визначити розташування джерела атаки по відношенню до локальної мережі (зовнішні або внутрішні атаки) [3, с. 122].

Як показала практика при використанні таких систем існує ряд проблем які істотно ускладнюють, а часом і зупиняють процес впровадження СВВ.

Фахівці в галузі інформаційної безпеки виділяють деякі з них, а саме:

– вимогливість до ресурсів і часом незадовільна продуктивність СВВ вже на 100 Мб/с мережах;

– недооцінка ризиків пов'язаних зі здійсненням мережних атак;

– невисока ефективність сучасних СВВ, що характеризується більшим числом помилкових спрацьовувань і неспрацьовувань (false positives and false negatives);

– недооцінка ризиків, пов'язаних зі здійсненням мережних атак;

– відсутність в організації методики аналізу й керування ризиками, що дозволяє адекватно оцінювати величину ризику й обґрунтовувати вартість реалізації контрзаходів для керівництва;

– висока вартість комерційних СВВ;

– висока кваліфікація експертів по виявленню вторгнень, що вимагає для впровадження й розгортання СВВ [3, с. 123].

На теперішній час для України є відносно невисока залежність підприємств від Інтернет. А також фінансування заходів щодо забезпечення інформаційної безпеки по залишковому принципу, не сприяє придбанню дорогих засобів захисту для протидії мережевим атакам.

Список бібліографічних посилань

1. Тулупов В. В., Спориш Е. С. Захист систем відеоспостереження від витоку інформації // Економічна та інформаційна безпека: проблеми та перспективи : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 27 квіт. 2018 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. С. 216-221.

2. Астахов А. IDS как средство управления рисками // Global Trust Solution. URL: http://www.globaltrust.ru/security/Pubs/Pub2_part5 (дата звернення: 12.10.2018).

3. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень. *Системи обробки інформації*. Харків : ХУПС. 2013. Вип. 6 (122). С. 122-123.

Одержано 30.10.2018

УДК 004.056.5

Ксенія Олександрівна КРАТАСЮК,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук,
доцент кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-3381-3350

ЗАХИСТ ОСОБИСТИХ ДАНИХ З ТЕХНОЛОГІЄЮ БЛОКЧЕЙН

Вступ і постановка проблеми.

Сучасні технології завдали відчутного удару по захисту нашої конфіденційної інформації. Велика частина того, чим займаються окремі особи або організації, стало надбанням громадськості. Сторонні особи беруть під контроль, зберігають і використовують особисті та корпоративні дані, шаблони, переваги і заняття. Багато нових бізнес-моделей ґрунтуються на зборі, організації та перепродажу наших особистих даних. Технології також спрощують пошук конкретної особи за його даними, навіть якщо цей користувач відмовився від