УДК 04.056:681.5.042
М. А. КАРПЕНКО, студентка;
О. В. КОЛОМІЄЦЬ, студент,
Державний університет телекомунікацій, Київ

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ В IoT ТА ЗАПОБІГАННЯ ЇМ

Розглянуто види сучасних систем виявлення вторгнень, що забезпечують захист інформаційних систем та мереж.

Ключові слова: IOT; аналіз; системи виявлення вторгнень; захист інформаційних систем та мереж; антивірусний захист.

Вступ

Способи захисту інформації на підприємстві, також як і канали витоку, постійно змінюються. З'являються нові пропозиції від різноманітних компаній, що надають послуги із захисту інформації. Панацеї звичайно немає, але є кілька базових кроків побудови системи захисту інформаційно-телекомунікаційної системи (ІТС) підприємства, на які необхідно обов'язково звернути увагу.

Багатьом напевно знайома концепція глибокого захисту від злому інформаційно-телекомунікаційної системи. Основна її ідея полягає в тому, щоб використовувати кілька рівнів захисту. Це дозволить мінімізувати збиток, пов'язаний із можливим порушенням периметра безпеки вашої ІТС.

Основна частина

Види захисту ІТС. До базового захисту ІТС підприємства належать:

1. *Firewall* (укр. *міжмережний екран*) — це програма або обладнання, яке перешкоджає зловмисникам і деяким типам шкідливих програм отримувати доступ до комп'ютера по мережі або через Інтернет. Для цього Firewall перевіряє дані, що надходять з Інтернету або по мережі, і блокує їх або дозволяє передачу на комп'ютер (рис. 1).

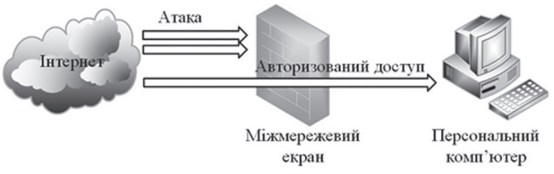

Рис. 1. Схема роботи міжмережного екрану

2. VPN (англ. *Virtual Private Network*, укр. *віртуальна приватна мережа*).

Віртуальна приватна мережа являє собою підімкнення типу «точка-точка» (логічне з'єднання), яка працює поверх приватної або публічної мережі.

VPN-підімкнення типу «мережа-мережа» (логічне з'єднання) дозволяють організаціям встановлювати маршрутизовані з'єднання між окремими офісами (або між іншими організаціями) по публічній мережі, при цьому забезпечуючи захищеність зв'язку (рис. 2) [2].

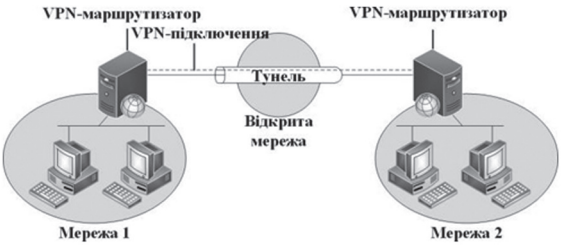

Рис. 2. Організація VPN-з'єднання двох віддалених вузлів

3. *IDS/IPS* (англ. *Intrusion Detection System/ Intrusion Prevention System*, укр. *система виявлення вторгнення (СВВ)/система запобігання вторгненню (СЗВ)*).

СВВ — програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого керування такою системою.

СЗВ — програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення.

Архітектуру СВВ і СЗВ наведено відповідно на рис. 3 і рис. 4 [1].

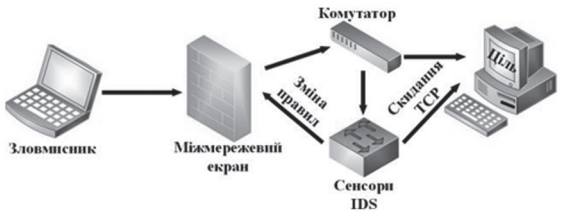

Рис. 3. Система виявлення вторгнень

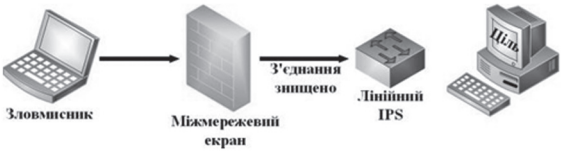

Рис. 4. Система запобігання вторгненням

4. *Антивірусний захист* — програмне забезпечення, яке здатне знаходити, «лікувати», блокувати, а також повністю видаляти віруси з системи.

Антивірусний захист здатний моментально попереджати про те, що на тій чи іншій веб-сторінці є вірус і ваша система може бути пошкоджена. Це дуже зручно, оскільки сама програма в цей самий час вживе всіх необхідних заходів. На даний момент існують багато різних програм антивірусного захисту, які різняться за ціною, швидкістю роботи, якістю антивірусних баз та іншими параметрами.

5. ***Білі списки*** — перелік певних програм та служб, які може використовувати користувач. Контролює білі списки адміністратор. Білі списки можна створити як за допомогою вбудованих засобів операційної системи, так і за допомогою стороннього програмного забезпечення.

6. ***Фільтрація спаму*** — процедура, яка перевіряє вхідну кореспонденцію (E-mail) за встановленими налаштуваннями фільтрів і забезпечує виявлення небажаної розсилки, яка може містити в собі рекламні пропозиції, «листи щастя», комп'ютерні віруси або бути спробою фішингу. До основних способів фільтрації спаму належать:

- спеціалізовані постачальники сервісів фільтрації спаму;
- програмне забезпечення для фільтрації спаму на власних поштових серверах.

7. ***Підтримання програмного забезпечення (ПЗ) в актуальному стані.*** Своєчасне оновлення ПЗ — це усунення вразливостей, виявлених у програмному продукті. Підтримання системи ПЗ в актуальному розробником стані — це робота в більш безпечному середовищі. У більшості систем передбачено механізм повного автоматичного оновлення.

8. ***Фізична та технічна безпека корпоративної мережі.*** Маючи фізичний доступ до мережного пристрою, зловмисник, здебільшого, легко отримає несанкціонований доступ до мережі підприємства. Забезпечення фізичної та технічної безпеки корпоративної мережі внеможливлює фізичний доступ до її складових [8].

Необхідно зауважити, що утримувати захист корпоративної мережі на високому рівні досить важко. Ви маєте бути впевнені, що компанія не залежить лише від одного-двох рубежів захисту. Завжди прагніть стежити за актуальною інформацією і свіжими вирішеннями на ринку інформаційної безпеки.

Система виявлення вторгнень (СВВ)

Системи виявлення вторгнень все частіше стають необхідним доповненням інфраструктури мережної безпеки. СВВ слугують механізмами моніторингу та спостереження щодо сумнівної активності. Вони можуть виявити нападників, які змогли обійти Firewall, і видати звіт щодо цього адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення вторгнень не роблять систему абсолютно безпечною. Як правило, СВВ мають таку структуру (рис. 5) [1].

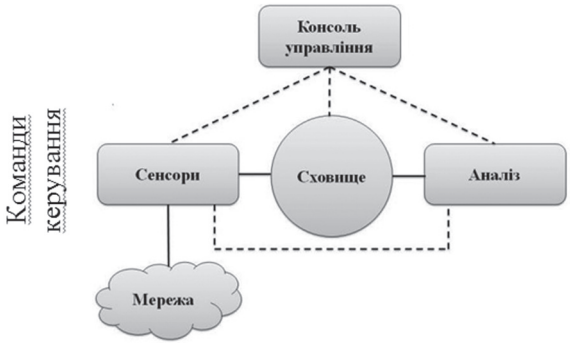

Рис. 5. Загальна структура СВВ

Сенсорна підсистема — відповідає за збір інформації, пов'язаної з безпекою мережі.

У ***сховищі*** зберігається інформація, що надходить від сенсорів й аналізатора.

Аналізатор — виявляє підозрілий трафік і атаки, ґрунтуючись на даних від сенсорів.

Консоль керування — дозволяє конфігурувати СВВ [5].

Класифікація СВВ

Архітектуру типових систем виявлення вторгнень зображено на рис. 6.

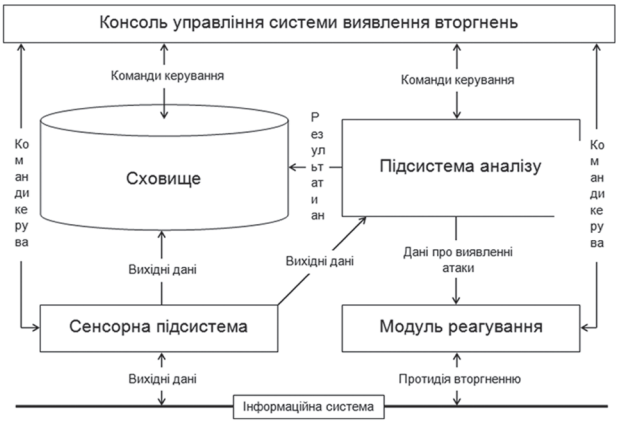

Рис. 6. Архітектура типових систем виявлення вторгнень

Основними компонентами систем виявлення вторгнень є сенсорна підсистема, підсистема аналізу, сховище, консоль керування та модуль реагування.

Сенсорна підсистема призначена для збору подій, пов'язаних із безпекою мережі або системи, що захищається.

Підсистема аналізу призначена для виявлення мережних атак і підозрілих дій.

Сховище, в якому нагромаджується база первинних подій і результати аналізу.

Консоль керування, що дає змогу конфігурувати СВВ, спостерігати за станом мережі або інформаційної системи та СВВ, переглядати виявлені

підсистемою аналізу інциденти несанкціонованих вторгнень.

Модуль реагування, який встановлено в сис- темах активної протидії, відповідає за виконання інструкцій щодо протидії несанкціонованому вторгненню в мережу або систему.

Системи виявлення вторгнень можна класифікувати так:

♦ ***За характером відповідної реакції:***

• *Пасивні* — системи виявлення, в яких після виявлення та розпізнавання підозрілого трафіку, СВВ тільки повідомляє користувача або адміністратора про загрозу;

• *Активні* — системи запобігання, що протистоять вторгненням шляхом скидання з'єднання або зміни правил Firewall з метою блокування підозрілого трафіку;

• *Гібридні*, що здійснюють виявлення та протистоять вторгненням в автоматичному режимі.

Сьогодні існує кілька різних типів СВВ систем, що відрізняються різними алгоритмами моніторингу даних і підходами до їх аналізу. Кожному виду системи відповідають ті чи інші особливості використання, переваги і недоліки.

Один із методів класифікації СВВ систем ґрунтується на з'ясуванні того, як вони здійснюють моніторинг інформаційної системи або мережі. Одні контролюють весь мережний трафік і аналізують мережні пакети, інші розгортаються на окремих комп'ютерах і контролюють операційну систему щодо виявлення ознак вторгнення.

♦ ***За способами моніторингу*** СВВ підподіляються на network-based (NIDS) і host-based (HIDS).

♦ ***За методиками аналізу*** — *статистичні* СВВ використовують статистичний підхід, після встановлення «навчаються» адміністратором, який задає політику СВВ, відповідну до нормальної активності в мережі — типи трафіку, з'єднання між вузлами, використовувані протоколи і порти. У разі виявлення аномалій у роботі мережі або статистично значущих відмінностей трафіку від типового в даній мережі, СВВ оповіщає про це адміністратора. Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибнопозитивних тривог у разі некоректно заданих правил. *Сигнатурні* СВВ аналізують трафік у мережі або порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). За такого підходу основною проблемою є старіння баз сигнатур. *Гібридна* СВВ поєднує два і більше підходів для розробки СВВ. Дані від агентів на хостах комбінуються з мережною інформацією для створення найбільш повного уявлення про безпеку мережі.

♦ ***За рівнем виявлення атак.***

Перевагами NIDS є велике покриття для моніторингу та у зв'язку з цим централізоване керування, також NIDS не впливають на продуктивність і топологію мережі. До недоліків цих систем належать: високе завантаження системи, NIDS потребує додаткового налаштування і функціональності мережних пристроїв. Системи NIDS не можуть аналізувати зашифровану інформацію і розпізнавати результати атак.

GrIDS (англ. *Graph-Based Intrusion Detection System*). Ця система є вдосконаленою версією NIDS. У кожний сегмент LAN встановлюється свій сніфер. Інформація від них збирається разом, аналізується і подається у вигляді схеми інформаційних потоків. Усі NIDS не залежать від типу використовуваної в мережі ОС. Для роботи їм необхідний виділений вузол у контрольованому сегменті і мережний адаптер, який уміє приймати всі типи пакетів. Логічним вирішенням буде встановлення захищеного з'єднання між NIDS і консоллю керування.

OIDS (англ. *Operational Intrusion Detection Systems*). Система спеціалізується на внутрішніх атаках. Ці системи розробили на випадок, якщо зловмиснику вдалося ввійти в систему від імені зареєстрованого користувача. Або коли атака на мережу відбувається зсередини її самої. Система порівнює дії конкретного користувача у даний момент часу з його звичайними діями, і у разі великих розбіжностей видає повідомлення. Простіше кажучи, оцінюється типовість дій (операцій) кожного з користувачів в той час, коли NIDS оцінює типовість трафіку.

HIDS (англ. *Host-based Intrusion Detection System*). Ця система працює з інформацією, зібраною всередині одного комп'ютера. Таке розташування дозволяє HIDS аналізувати діяльність із великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають відношення до конкретної атаки в ОС. HIDS зазвичай використовують інформаційні джерела двох типів: результати аудиту ОС і системних журналів подій. HIDS мають можливість стежити за подіями локально, відносно хоста, можуть визначати атаки, які не можуть виявити NIDS. HIDS можуть функціонувати в системі, в якій мережний трафік зашифровано, і система не вимагає додаткової функціональності мережних пристроїв. До недоліків цієї системи належить: високе завантаження системи хоста, мале покриття для моніторингу, не мають централізованого керування і можуть бути блокованими деякими DoS-атаками або навіть заборонені.

ERIDS (англ. *External Routing Intrusion Detection System*). Приклад інноваційної та вузькоспеціалізованої системи. Необхідність її створення було зумовлено тим фактом, що крім простого і розподіленого способу збору даних про мережі існують менш тривіальні. Наприклад, зло-

вмисник спочатку здійснює атаку на маршрутизатор, змінює його налаштування у такий спосіб, що він направляє трафік через сегмент, який не контролюється і доступний атакуючому [3].

Інфраструктура хостинг-провайдера з використанням IDS

Для забезпечення інформаційної безпеки ІТС хостинг-провайдера необхідно реалізувати механізми захисту в системі.

Схему мережі хостинг-провайдера зображено на рис. 7.

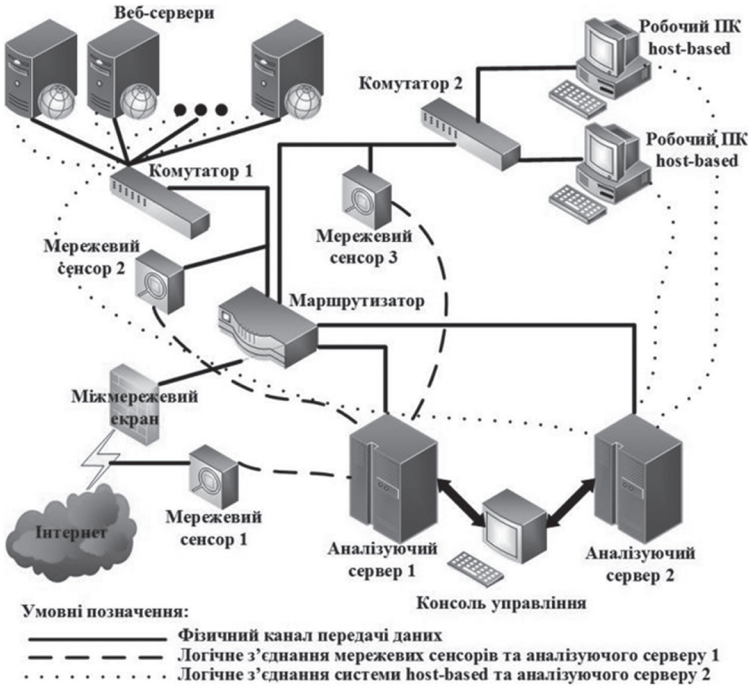

Рис. 7. Схема мережі хостинг-провайдера

У мережі хостинг-провайдера використовують комбінацію з мережної та хостової СВВ. Систему NIDS розміщено на окремій системі, яка відстежує мережний трафік на наявність проявів атак, які відбуваються у підконтрольному сегменті системи [4].

Існує п'ять основних типів сенсорів HIDS:

1) аналізатори журналів;
2) сенсори ознак;
3) аналізатори системних викликів;
4) аналізатори поведінки програм, служб;
5) контролери цілісності файлів.

Слід зауважити, що деякі розробники ПЗ пропонують нові функціональні можливості сенсорів HIDS.

Під час розміщення сенсорів NIDS необхідно керуватися ще одним ключовим правилом. Якщо в мережі використовуються комутатори замість концентраторів, то сенсор виявлення вторгнень не буде правильно працювати, якщо його просто підімкнено до порту комутатора. Комутатор буде відправляти тільки трафік, спрямований на сенсор, до того порту, до якого підімкнено сенсор. У разі комутованої мережі існують два варіанти використання сенсорів виявлення вторгнень: застосування порту, що відстежує комутатор, або застосування мережного розгалужувача.

Найбільш популярними системами з відкритим кодом є Snort, Suricata і OSSEC HIDS, з пропрієтарним кодом CATNET і McAfee IPS, Cisco Secure IDS, Dragon IDS [6].

Для захисту веб-сторінок від НСД необхідно реалізувати функціональні послуги безпеки інформації згідно з НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

Для технології Т2{КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1} системи IDS дозволяють реалізувати частину критеріїв, використовуючи свої механізми аналізу інформації, яка циркулює в ІТС провайдера [7].

Висновки

Отже, зважаючи на особливості систем виявлення вторгнень та детально ознайомившись із недоліками та перевагами обох видів даних систем, можна дійти висновку, що найкращим захистом для інформаційної системи з'єднання або частини ЗС України буде гібридне використання одночасно обох видів систем IDS в одній інформаційній мережі.

Такий метод дасть змогу надійно захистити інформаційну систему, використовуючи всі переваги систем виявлення вторгнень. Але варто пам'ятати, що системи IDS це лише один з інструментів захисного арсеналу і він не повинен розгля-

датися як заміна для будь-якого з інших захисних механізмів. Захист інформації найбільш ефективний, коли в мережі підтримується багаторівневий захист.

Сучасні системи забезпечення інформаційної безпеки корпоративної мережі підприємства дають можливість обрати найбільш вдалий та дієвий спосіб захисту інформації, яка циркулює в ІТС. Враховуючи це, власник ІТС має можливість вибрати, відповідно до свого бюджету, необхідні механізми захисту, починаючи від антивірусного ПЗ, закінчуючи системами виявлення вторгнень та запобігання їм. Кінцевою метою власника ІТС є розробка комплексної системи захисту інформації, яка забезпечить надійний захист інформації з обмеженим доступом.

Список використаної літератури

*1. **Многоагентные** технологии комплексной защиты информации в телекоммуникационных системах / В. И. Городецкий, И. В. Котенко, О. В. Карсаев, А. В. Хабаров // Труды 7-й междунар. конф. по информационным сетям и системам ISINAS – 2000 (октябрь). СПб., 2000. С. 122–134.*

*2. **Scarfone Karen.** Guide to Intrusion Detection and Prevention Systems (IDPS). 2007. 127 p.*

*3. **Сайт** http://netconfig.ru/ [Електронний ресурс]. URL:*

http://netconfig.ru/ server/ids-ips/

*4. **Sen Sevil.** Power-Aware Intrusion Detection in Mo- bile Ad Hoc Networks. 2006.*

*5. **Anderson Ross.** Security Engineering: A Guide to Building Dependable Distributed Systems. 2007. 388 p.*

*6. **Jackson Kathleen.** A Phased Approach to Network Intrusion Detection. 1991. 30 p.*

*7. **Syngress.** Snort IDS and IPS Toolkit. 2007. 197 p.*

*8. **ДСТСЗІ** СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу». 2003. 16 с.*

*9. **Грайворонський М. В., Новіков О. М.** Безпека інформаційно-комунікаційних систем. 2009. 608 с.*

Рецензент: канд. техн. наук **В. Р. Косенко**, Державний університет телекомунікацій, Київ.

М. А. Карпенко, А. В. Коломиец

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ В IoT

Рассмотрены виды современных систем обнаружения вторжений, обеспечивающих защиту информационных систем и сетей.

Широко известна концепция глубокой защиты от взлома информационно-телекоммуникационной системы. Основная ее идея состоит в том, чтобы использовать несколько уровней защиты. Это позволит минимизировать ущерб, связанный с возможным нарушением периметра безопасности ИТС.

Учет всех особенностей систем обнаружения вторжений и детальный анализ недостатков и преимуществ различных систем привел к выводу, что лучшей защитой для информационной системы будет гибридное использование одновременно двух видов систем IDS в одной информационной сети.

Ключевые слова: IoT; анализ; системы выявления вторжений; защита информационных систем и сетей; антивирусная защита.

M. A. Karpenko, O. V. Kolomiets

ANALYSIS OF MODERN SYSTEMS FOR DETECTING AND PREVENTING INTRUSIONS TO IoT

The article discusses the types of modern intrusion detection systems that protect information systems and networks.

The concept of deep protection against hacking of an information and telecommunication system is widely known. Its main idea is to use several levels of protection. This will minimize the damage associated with a possible violation of the ITS security perimeter.

Taking into account all the features of intrusion detection systems and a detailed analysis of the disadvantages and advantages of various systems has led to the conclusion that the best protection for an information system will be the hybrid use of two types of IDS systems simultaneously in one information network.

Key words: IoT; analysis; intrusion detection systems; protection of information systems and networks; antivirus protection.