УДК 621.396 **doi: 10.26906/SUNZ.2022.2.059**

А. С. Янко, О. І. Макаренко

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

КОНЦЕПЦІЯ СИСТЕМИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ ДО МЕРЕЖІ

Анотація. Виявлення та запобігання мережевих атак є одним з найважливіших завдань системи безпеки мережі. Дана стаття присвячена захисту комп'ютерних мереж від атак, вторгнень та несанкціонованого доступу. Особлива увага приділяється принципу роботи мережевих систем виявлення та запобігання вторгнень. Розглянуто поведінкову аналітику користувачів і об'єктів UEBA для виявлення порушень в області безпеки. На прикладі центру безпеки Azure досліджується інтелектуальні засоби безпеки і розширення аналітики для швидшого виявлення загроз і зменшення кількості неправдивих оповіщень. На основі розглянутої концепції виявлення та запобігання вторгнень можливо побудувати ефективну систему сповіщення за захисту мереж.

Ключові слова: активний мережевий сенсор, інформаційна безпека, комп'ютерна мережа, мережеві системи виявлення вторгнень, несанкціонований доступ, система запобігання вторгнень.

Вступ

Виявлення мережевих атак є в даний момент одним з найбільш гострих проблем безпечного застосування корпоративних мереж. Масштабні епідемії мережевих черв'яків, автоматизовані засоби пошуку вразливості мереж – усе це робить забезпечення безпеки локальних мереж дуже трудомісткою справою. Зараз важко знайти мережу, в якій відсутні такі активні засоби попередження атак як антивірус, брандмауер, системи попередження та виявлення вторгнень. На жаль, одних активних засобів відображення атак недостатньо. Тому, на додаток до них застосовують пасивні засоби боротьби з атаками – мережеві системи виявлення вторгнень.

Мережеві системи виявлення вторгнень (МСВВ) переглядають увесь мережевий трафік (чи трафік певної ділянки мережі) і при виявленні якихнебудь відхилень у ньому сигналізують про це. Формальні МСВВ використовують сигнатурні правила – пакети, що потрапляють на сенсори, порівнюються з БД сигнатур і, у разі виявлення збігу, оголошується тривога. На жаль, навіть формальних МСВВ стає недостатньо для надійного захисту мережі. За даними CERT, кількість відомих нових методів вторгнення тільки за 2010 рік перевищила 25000. Це означає, що в середньому, щодня з'являється близько 70 нових атак. Фізично неможливо оновлювати БД сигнатур формальних МСВВ за такі проміжки часу. Крім того, збільшення об'єму сигнатур негативно позначається на продуктивності систем.

Аналіз останніх досліджень і публікацій. В сучасних дослідженнях спостерігаються два підходи до створення систем захисту інформації. Перший підхід передбачає реалізацію заходів, спрямованих на запобігання несанкціонованим впливам порушника на інформаційну сферу комп'ютерної мережі. При цьому підході до структури системи включаються міжмережеві екрани, засоби контролю доступу та аналізу захищеності [1, 2]. Другий підхід ґрунтується на виявлення факту несанкціонованого проникнення порушника, а також на локалізації місця та встановлення джерела впливу. Основу структури системи складають засоби виявлення несанкціонованих впливів, здатних фіксувати спроби порушення інформаційної безпеки на початковому етапі їх розвитку.

В розглянутих підходах відсутні засоби, які б одночасно поєднувати у собі всі інформаційні характеристики систем захисту мережі. Для створення інтегрованих систем захисту з усіма функціональними характеристиками вище розглянутих підходів, доцільно включити до структури системи наступні компоненти: засоби виявлення несанкціонованого доступу (мережевий сенсор та детектори), засоби аналізу захищеності, спеціалізовані програмно-апаратні засоби захисту тощо.

Метою статті є підвищення інформаційної безпеки комп'ютерних мереж на основі створення надійної мережевої системи виявлення вторгнень, як ефективного елементу інтегрованої системи захисту.

Виклад основного матеріалу

Можливості виявлення. Нинішній ландшафт загроз вимагає нового підходу до систем виявлення, що спирається на традиційну складність тонкого налаштування початкових правил, порогових значень, базових показників. Боротьба з множиною хибних спрацьовувань стає неприйнятною для багатьох організацій.

При підготовці до захисту від зловмисників команда повинна використовувати ряд методів, які включають в себе:

- кореляцію даних з декількох джерел;
- профілізація;
- поведінкова аналітику;
- виявлення аномалій;
- оцінку активності;
- машинне навчання.

Важливо підкреслити, що деякі традиційні засоби управління безпекою, такі як аналіз протоколів та антивірусне ПЗ на основі сигнатур, все ще займають свою нішу на лінії захисту, але призначені для боротьби із застарілими загрозами. Ви не повинні видаляти своє антивірусне програмне забезпечення тільки тому, що воно не володіє можливостями машинного навчання. Це все ще рівень захисту вашого хоста.

З іншого боку, традиційне мислення захисника, яке фокусується тільки на моніторингу користувачів з великими повноваженнями, закінчилося, і у вас більше не може бути такого підходу. Для виявлення поточних загроз необхідно переглядати облікові записи усіх користувачів, профілювати їх і розуміти звичайну поведінку.

Діючі суб'єкти загроз намагатимуться скомпрометувати звичайного користувача, залишитися в мережі і продовжувати вторгнення шляхом подальшого поширення і збільшення привілеїв. З цієї причини у вас мають бути механізми виявлення, які могли б ідентифікувати таку поведінку на усіх пристроях, в різних місцях і створювати сповіщення на основі кореляції даних, як показано на рис. 1.

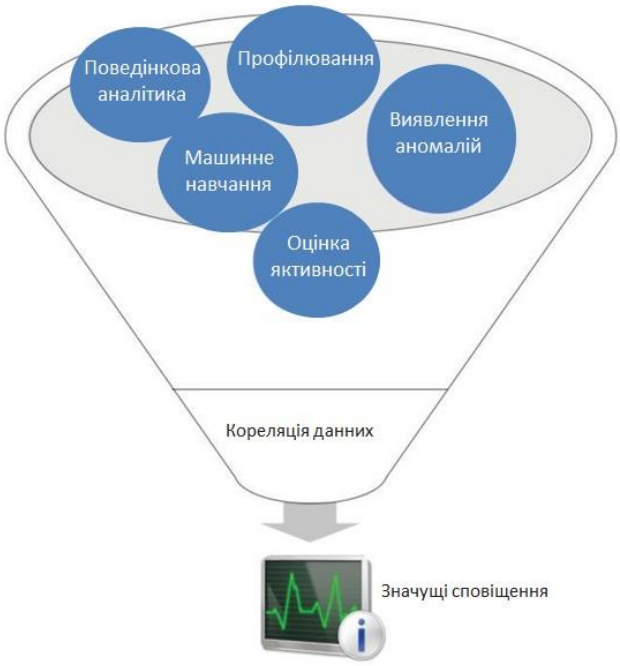

Рис. 1. Процес кореляції даних та сповіщення

Коли контекстуалізуються дані, то природним чином зменшується кількість хибних спрацьовувань, що дає значущий результат для системи безпеки.

Індикатори компрометації. Говорячи про виявлення, важливо згадати про індикатори компрометації. Коли нові загрози виявляються в природному середовищі, у них зазвичай є якийсь поведінковий шаблон і вони залишають свій слід в системі жертви.

Наприклад, програма-вимагач Petya виконала наступні команди в цільовій системі, щоб перепланувати перезапуск:

schtasks /Create /SC once /TN "" /TR "<systemfolder>shutdown.exe /r /f" /ST <time> cmd.exe /c schtasks /RU "SYSTEM" /Create /SC once /TN "" /TR "C:Windowssystem32shutdown.exe /r /f" /ST <time>

Ще одним індикатором дії цієї програми є сканування локальної мережі через порти TCP 139 і TCP 445. Це важливі ознаки того, що в цільовій системі відбувається атака, а винуватець – Petya. Системи знаходження зможуть збирати ці індикатори компрометації і видавати сповіщення при здійсненні атаки. Використовуючи Azure Security Center як приклад, через деякий час після виявлення загрози Petya центр автоматично оновлює свій механізм захисту і може попередити користувачів про те, що їх комп'ютер був скомпрометований, як показано на рис. 2.

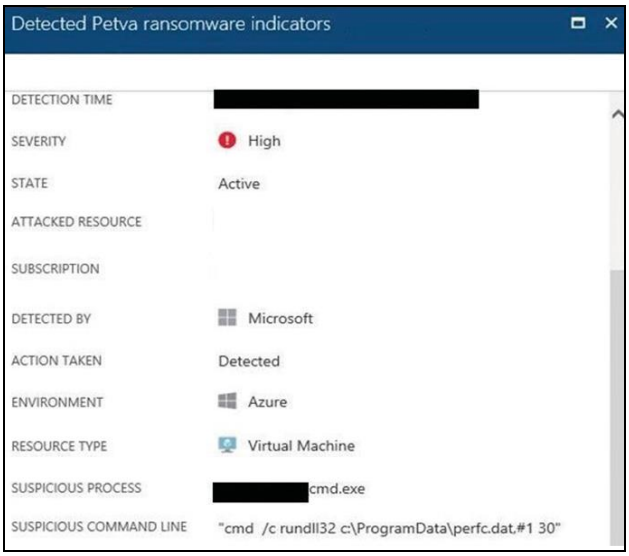

Рис. 2. Виявлення вірусу Petya
за допомогою Azure Security Center

Ви можете зареєструватися на сайті OpenIOC (**http://openioc.org**), щоб отримати інформацію про нові індикатори, а також внести свій вклад в суспільство.

Використовуючи IOCEditor (зверніться до довідкового розділу, де вказаний URL- адреса, з якої його можна завантажити), ви можете створити свій власний індикатор або проглянути вже існуючий.

Система виявлення вторгнень. Як випливає з назви, система виявлення вторгнень (СВВ, Intrusion Detection System – IDS) відповідає за виявлення потенційного вторгнення та ініціацію сповіщення. Що можна зробити з цим сповіщенням, залежить від політики системи виявлення [3]. При створенні політики СВВ необхідно відповісти на наступні питання:

- Хто повинен контролювати СВВ?
- У кого має бути доступ з правами адміністратора СВВ?
- Як оброблятимуться інциденти на основі сповіщень, згенерованими СВВ оцінку активності?
- Яка політика оновлення СВВ?
- Де треба встановити СВВ?

Це лише деякі приклади первинних питань, які повинні допомогти в плануванні прийняття СВВ. При пошуку СВВ також можна звернутися до списку постачальників в ICSA Labs (www. icsalabs.com) для отримання додаткової інформації про постачальника.

Незалежно від бренду типова система виявлення вторгнень володіє можливостями, показаними на рис. 3.

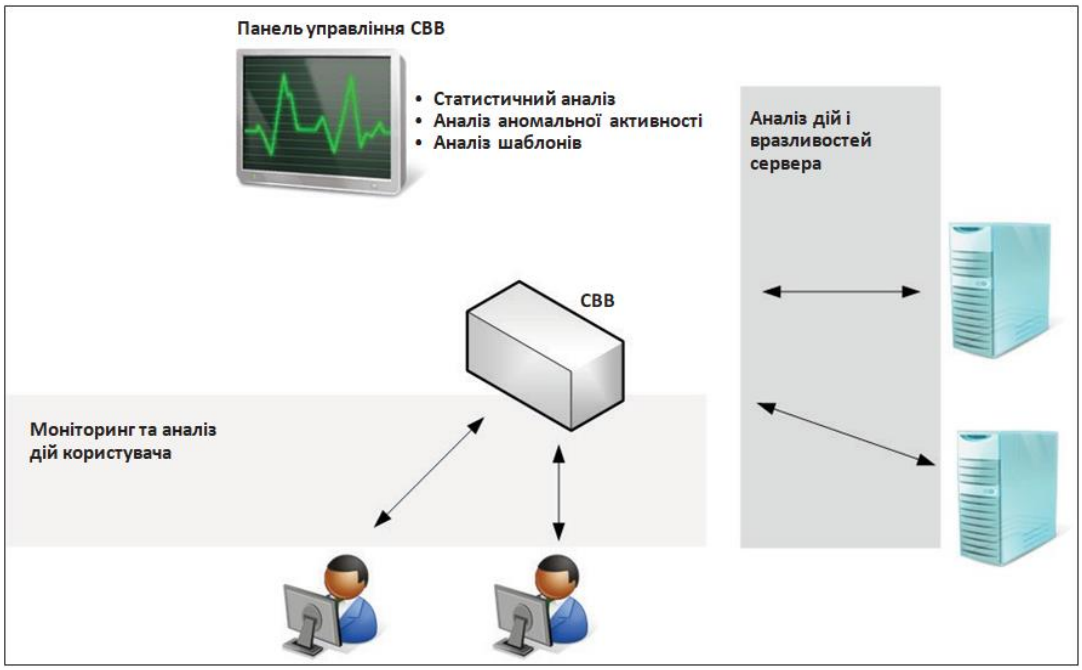

Рис. 3. Схема СВВ

Хоча це основні можливості, кількість функцій насправді залежатиме від постачальника і методу, використовуваного СВВ. Система виявлення вторгнень на базі сигнатур проситиме базу даних про сигнатури (слідах) вже відомих атак і відомих системних вразливостей, щоб перевірити, чи являється те, що було виявлено, загрозою і чи повинне спрацювати сповіщення. Оскільки це база цих сигнатур, вона вимагає постійного оновлення, щоб мати в розпорядженні останню версію. Ґрунтована на поведінці СВВ працює, створюючи базові шаблони, на основі того, що вона дізналася від системи. Вивчивши нормальну поведінку, стає легше виявляти відхилення.

Система виявлення вторгнень також може базуватися на окремій машині, коли механізм СВВ виявлятиме спробу вторгнення тільки на конкретний хост, або це може бути МСВВ, яка визначає вторгнення для сегменту мережі, в якому встановлена МСВВ. Це означає, що у випадку з МСВВ розміщення стає критично важливим для збору цінного трафіку. Саме тут команда повинна тісно співпрацювати з командою IT-інфраструктури, щоб забезпечити установку системи виявлення вторгнень в стратегічно важливих місцях по усій мережі. При плануванні розміщення МСВВ встановіть пріоритетність наступних сегментів мережі:

- ДМЗ/периметр;
- основна корпоративна мережа;
- бездротова мережа;
- мережа віртуалізації;
- інші критичні сегменти мережі.

Ці сенсори прослуховуватимуть трафік, а це означає, що вони не споживатимуть надто багато пропускної спроможності мережі.

На рис. 4 наведений приклад розміщення СВВ. Зверніть увагу, що в цьому випадку система виявлення (яка на справді в даному випадку є МСВВ) була додана до кожного сегменту (використовуючи SPAN-порт на мережевому комутаторі). *Система запобігання вторгень***.** Система запобігання вторгнень (СЗВ, Intrusion Prevention System – IPS) використовує ту ж концепцію СВВ, але, як випливає з назви, вона запобігає вторгненню, роблячи дії, що коригують. Ці дії будуть налагоджені адміністратором СЗВ.

Подібно до того як СВВ доступна для хостів (ХСВВ) і мережі (МСВВ), СЗВ так само доступна для хостів (ХСЗВ) і мережі (МСЗВ). Розміщення МСЗВ у вашій мережі має вирішальне значення, і тут застосовані ті ж рекомендації, що були згадані раніше. Також слід розглянути можливість розміщення МСЗВ відповідно до трафіку, щоб при необхідності робити коригуючи дії. СЗВ зазвичай може працювати в одному або декількох з наступних режимів: на основі правил або на основі аномалій.

Виявлення на основі правил. При роботі в цьому режимі СЗВ порівнює трафік з набором правил і намагається перевірити, чи відповідає трафік правилу. Це дуже корисно, коли вам потрібно розгорнути нове правило, щоб заблокувати спробу експлуатації вразливостей.

Системи МСЗВ, такі як Snort, здатні блокувати загрози, використовуючи виявлення на основі правил [4].

Наприклад, правило Snort Sid 1-42329 здатне виявити різновид Win.Trojan.Doublepulsar.

Правила Snort знаходяться тут: etc/snort/rules, а інші правила можна завантажити за адресою https://www.snort.org/downloads/#rule-downloads.

Іноді для нейтралізації загрози потрібно декілька правил. Наприклад, правила 42340 (спроба доступу до IPC- ресурсу анонімного сеансу протоколу SMB), 41978 (спроба видаленого виконання коду протоколу SMB) і 42329-42332 (різновид Win.Trojan.Doublepulsar) можуть бути використані для виявлення програми-вимагача WannaCry.

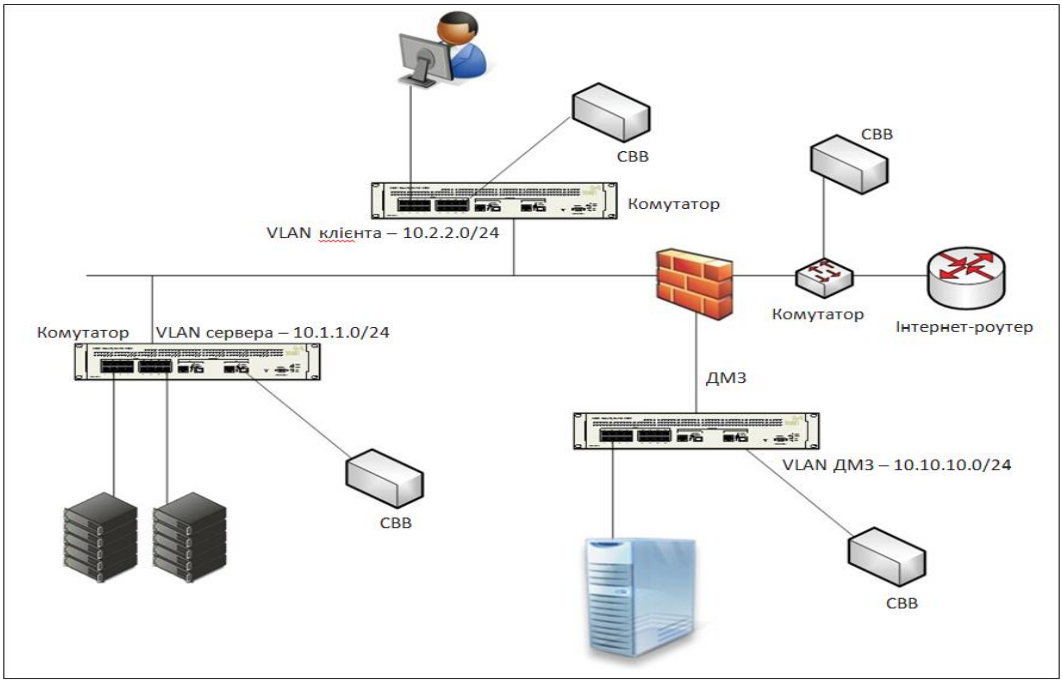

Рис. 4. Схема СЗВ

Перевага використання МСЗВ з відкритим початковим кодом, такий як Snort, полягає в тому, що коли нова загроза стає доступною в мережі, співтовариство зазвичай досить швидко реагує, публікуючи нове правило для виявлення загрози. Наприклад, коли був виявлений вірус-вимагач Petya, співтовариство створило правило і розмістило його на GitHub (його можна побачити тут: https://goo.gl/mLtnFM). Хоча постачальники і співтовариство безпеки дійсно швидко публікують нові правила, ви повинні стежити за новими індикаторами компрометації і створювати правила МСЗВ на їх основі.

Виявлення на основі аномалій. В цьому випадку аномалія ґрунтована на тому, що СЗВ класифікує як аномальне. Ця класифікація зазвичай ґрунтована на евристиці або зведенні правил. Один з варіантів – статистичне виявлення аномалій, при якому беруться вибірки мережевого трафіку у випадкові моменти часу і виконується порівняння з базовим станом. Якщо цей зразок виходить за межі базового стану, вирушає сповіщення з подальшою дією.

Поведінкова аналітика всередині організації. Для переважної більшості компаній, що знаходяться на ринку нині, основний бізнес як і раніше здійснюється усередині організації. Це місце, де знаходяться критично важливі дані, працюють більшість користувачів та знаходяться ключові ресурси. Як ви знаєте, ми розглядали стратегії атаки в першій частині цієї книги.

У зловмисників існує тенденція мовчки проникати у вашу локальну мережу, поширюватися далі, підвищувати привілеї і підтримувати зв'язок з командно-контрольним сервером, поки він не зможе виконати свою місію. З цієї причини наявність аналітики поведінки потрібна, щоб швидко розірвати життєвий цикл атаки [5].

На думку компанії Gartner, дуже важливо зрозуміти, як поводяться користувачі. Відстежуючи легітимні процеси, організації можуть використати поведінкову аналітику користувачів і об'єктів (User and Entity Behavior Analytics – UEBA) для виявлення порушень в області безпеки. Використання UEBA для виявлення атак дає багато переваг, але одними з найбільш важливих є можливість виявлення атак на ранніх етапах і вжиття заходів, що коригували, для стримування атаки.

На приведеному нижче рис. 5 показаний приклад того, як UEBA переглядає різні об'єкти, щоб прийняти рішення, повинно спрацювати сповіщення або ні.

Без системи, яка може дивитися усі дані в широких масштабах і робити кореляції не лише за шаблоном трафіку, але і за профілем користувача, шанси неправдивого спрацьовування зростають. Наприклад, коли є система UEBA усередині організації. Система знає, до яких серверів зазвичай звертаються користувачі, які ресурси відвідують, яку операційну систему використовують для доступу до цих ресурсів, а також їй відоме географічне місце розташування користувачів. На рис. 6 показаний приклад цього типу виявлення, отриманого від Advanced Threat Analytics (ATA) компанії Microsoft, яка використовує поведінкову аналітику для виявлення підозрілої поведінки. Зверніть увагу, що в цьому випадку повідомлення досить чітке. В ньому говориться, що адміністратор не виконував ці дії минулого місяця, в результаті дані не корелюють з іншими обліковими записами в організації.

Це попередження не можна ігнорувати, тому що воно контекстуалізовано, а це означає, що аналізує дані, зібрані під різними кутами, щоб виконати зіставлення і прийняти рішення про те, чи треба видавати сповіщення чи ні.

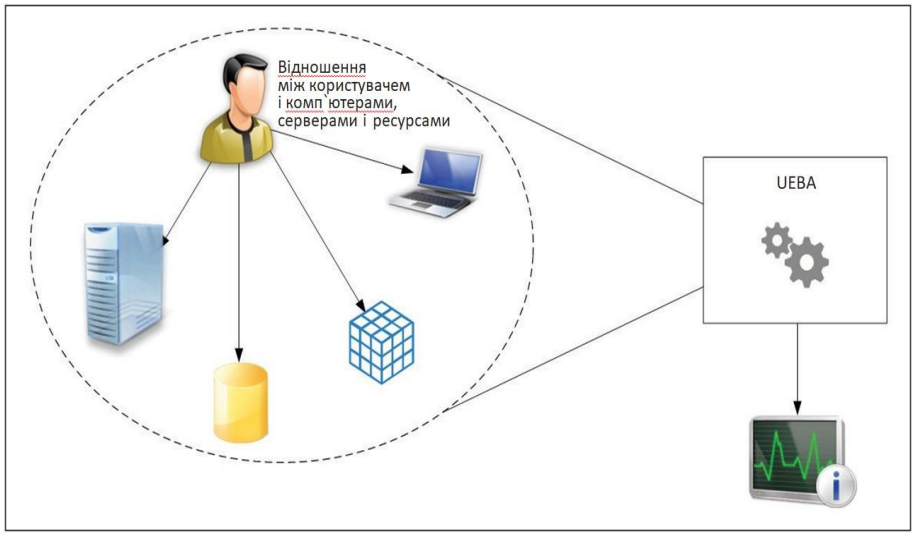

Рис. 5. Принцип роботи UEBA

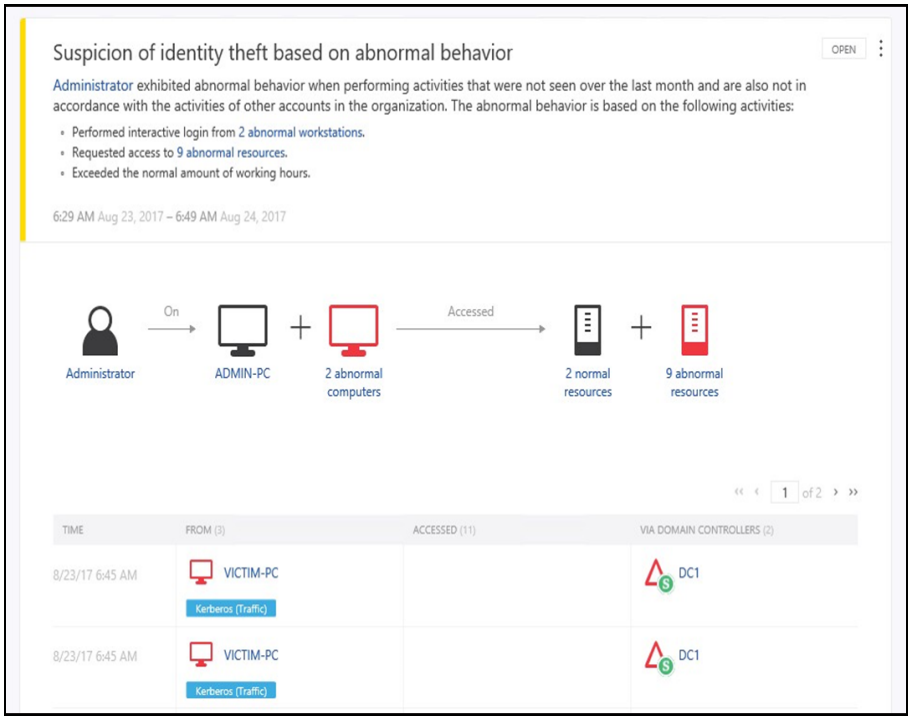

Рис. 6. Виявлення підозрілої поведінки користувача

Система UEBA всередині організації може допомогти команді проявити велику активність і отримати відчутніші дані для точного реагування. Система UEBA складається з декількох модулів, і ще один модуль - це розширене виявлення загроз, яке шукає відомі уразливості і шаблони атак. На рис.7. показано, як Microsoft ATA виявляє атаку Pass-the-ticket.

Оскільки існують різні способи виконання цієї атаки, розширене виявлення загроз не може шукати тільки сигнатуру, повинне шукати схему атаки і те, що намагається зробити зловмисник. Це набагато ефективніше, чим використати систему на базі сигнатур.

Також здійснюється пошук підозрілу поведінку, яка йде від звичайних користувачів, які не повинні виконувати певні завдання. Наприклад, якщо звичайний користувач намагається запустити NetSess.exe в локальному домені, Microsoft ATA розглядає це як перебір SMB-сесій, що, з точки зору зловмисника, як правило, здійснюється на етапі розвідки. З цієї причини Microsoft ATA видає попередження про намагання користувача запустити NetSess.exe.

Зловмисники не лише будуть використовувати вразливості, але і скористаються помилковими конфігураціями в системі, на яку вони націлилися, такими як неправильна реалізація протоколу і відсутність захисту. З цієї причини система UEBA також виявить системи, в яких відсутня безпечна конфігурація. На рис. 8 показано, як Microsoft ATA виявляє службу, що надає доступ до облікових даних акаунту, оскільки вона використовує протокол LDAP без шифрування.

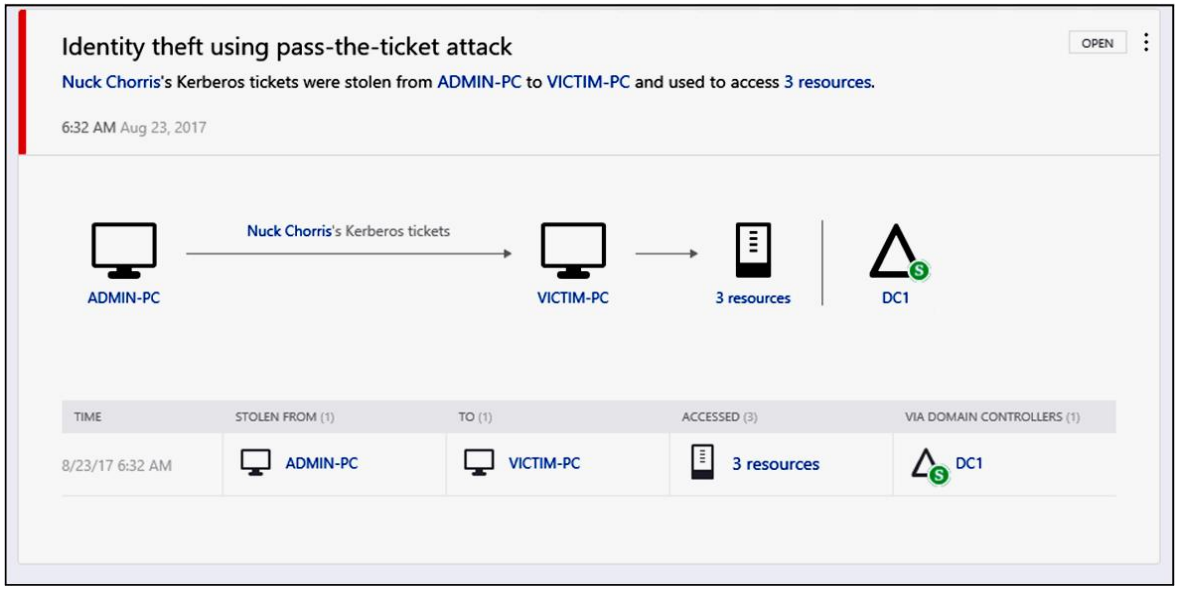

Рис. 7. Виявлення атаки Pass-the-ticket за допомогою Microsoft ATA

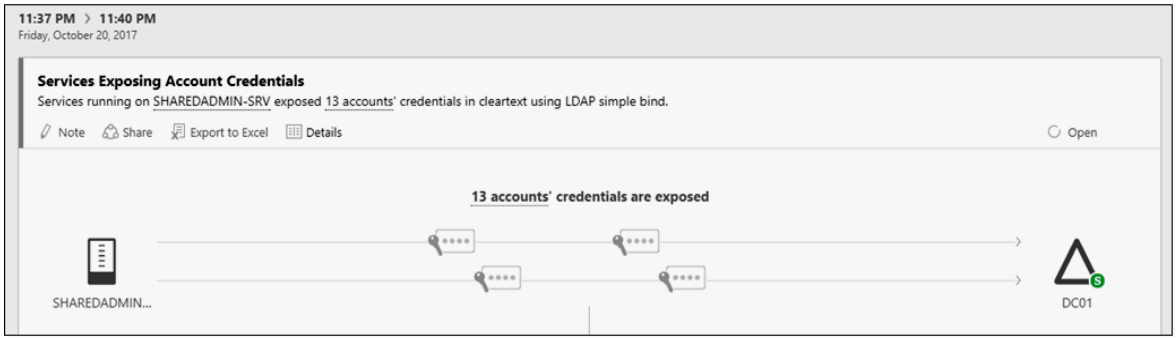

Рис. 8. Попередження програми Microsoft ATA

Центр безпеки Azure. Центр безпеки використовує інтелектуальні засоби безпеки і розширену аналітику для швидшого виявлення загроз і зменшення кількості неправдивих спрацьовувань. В ідеалі будите використовувати систему одного вікна для візуалізації сповіщень і підозрілих дій на усі робочих навантаженнях. Основна топологія виглядає аналогічно тій, що показана на рис. 9.

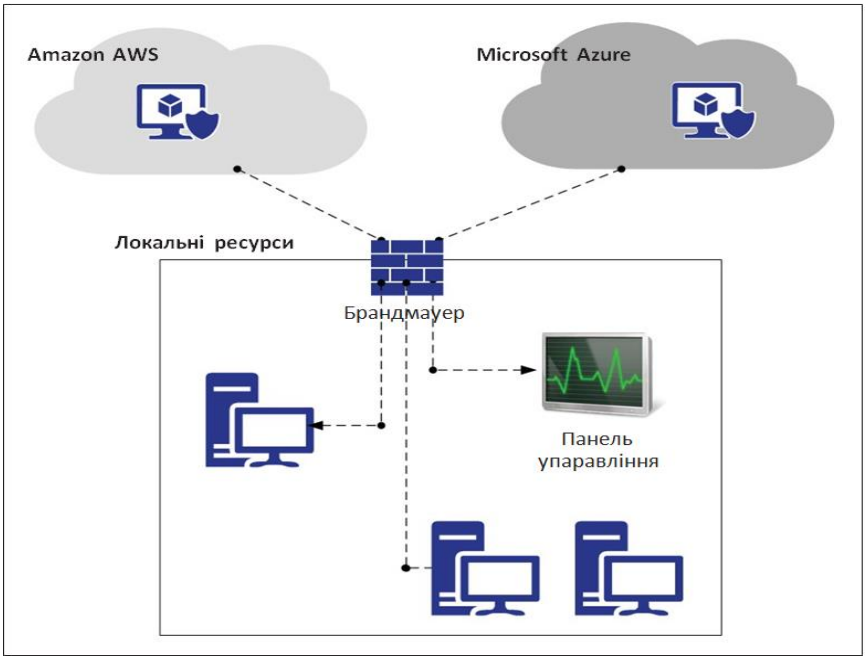

Рис. 9. Топологія Microsoft Azure

Коли центр безпеки буде встановлений на цих комп'ютерах, він збиратиме:

- трасування ETW (Event Tracing for Windows),
- події журналів операційної системи,
- запущені процеси,
- ім'я комп'ютера,
- IP-адреси,

зареєстрованих користувачів.

Ці події вирушають в Azure і зберігаються у вашому особистому сховищі робочого простору. Центр безпеки проаналізує ці дані, використовуючи такі методи, як:

- кіберрозвідка;
- поведінкова аналітика;
- виявлення аномалій.

Після оцінки цих даних Центр безпеки запустить сповіщення на основі пріоритету і додасть це на панель моніторингу, як показано на наведеному нижче рис. 10.

Рис. 10. Панель сповіщень Azure

Зверніть увагу що перше сповіщення має інший значок і називається Security Incident Detected (виявлений інцидент у сфері безпеки).

Відбувається це тому, що він був ідентифікований, а дві або більше атаки є частиною однієї і тієї ж компанії, спрямованої проти певного ресурсу.

Це означає, що, центр безпеки збирає дані з метою знайти взаємозв'язок між подіями, він робить це автоматично і надає відповідні сповіщення для аналізу.

Коли натиснути на це сповіщення, з'явиться наступне вікно (рис. 11).

У нижній частині цієї сторінки видно усі три атаки (в порядку їх виникнення) на BM1 і рівень серйозності, призначений центром безпеки.

Приведемо одно важливе спостереження відносно переваги використання поведінкової аналітики для виявлення загроз. Йдеться про третє по рахунку сповіщення Multiple Domain Accounts Queried (Запит декількох облікових записів домена). Команда, яка була виконана, щоб видати це сповіщення: netuser<username> /domain.

Проте, щоб прийняти рішення про те, що це виглядає підозріло, необхідно подивитися на нормальну поведінку користувача, який виконав цю команду, і зіставити цю інформацію з іншими даними, які при аналізі в контексті будуть віднесені до категорії підозрілих. Як видно з цього прикладу, хакери використовують вбудовані системні інструменти та інтерфейс типу «native» командного рядка для виконання своєї атаки. З цієї причини вкрай важливо мати в наявності інструмент логування викликів з командного рядка.

Центр безпеки також використовуватиме статистичне профілювання для побудови традиційних базових показників і сповіщення про відхилення, які відповідають потенційному вектору атаки. Це корисно у багатьох сценаріях.

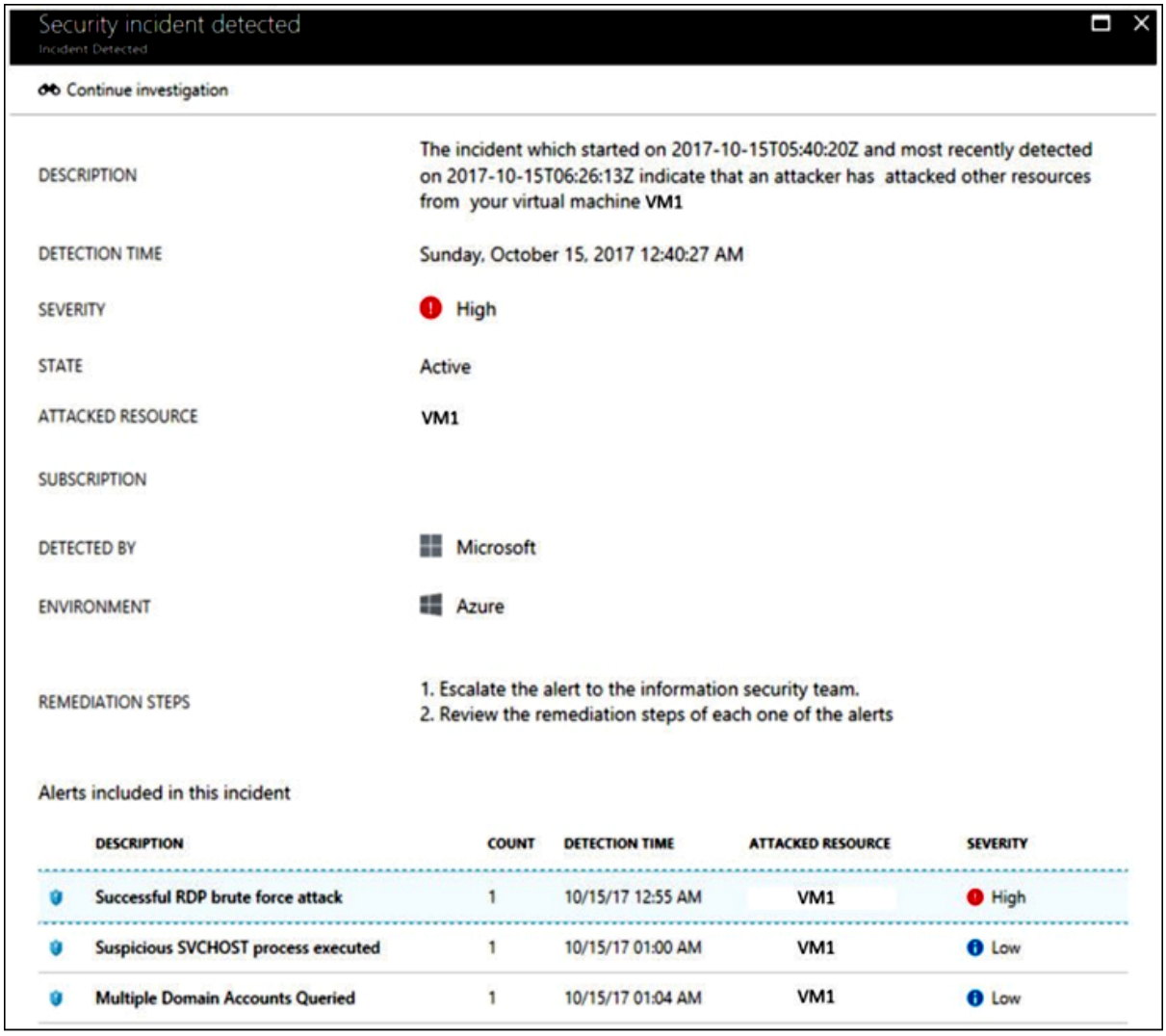

Рис. 11. Інформація про сповіщення в Azure

Типовий приклад – відхилення від нормальної діяльності.

Наприклад, припустимо, що хост запускає підключення по RDP 3 рази в день, але в певний день робиться сотня спроб. Коли таке відхилення відбувається, має бути видане сповіщення, щоб попередити про це.

Ще одним важливим аспектом роботи з хмарним сервісом є вбудована інтеграція з іншими постачальниками.

Центр безпеки може інтегруватися з багатьма іншими рішеннями, такими як Barracuda, F5, Imperva і Fortinet для брандмауера веб-застосувань, серед інших для захисту кінцевих точок, оцінки вразливостей і брандмауера наступного покоління.

Приведене на рис. 12 зображення показує приклад такої інтеграції.

Зверніть увагу, що це сповіщення було згенероване Deep Security Agent, і оскільки воно інтегроване з центром безпеки, то відображатиметься на тій же панелі моніторингу, що і інші події, виявлені центром безпеки.

Треба запам`ятати, що центр безпеки – це не єдине рішення, яке здійснюватиме моніторинг системи та інтегруватиметься з іншими постачальниками. Існує безліч SIEM (Security Information and Event Management) – рішень для забезпечення безпеки інформації і управління подіями, таких як Splunk і LogRhythm, які виконуватимуть моніторинг аналогічного типу.

Висновки

Виявлення та запобігання мережевих атак є одним з найважливіших завдань системи безпеки мережі.

В даній статті було розглянуто різні типи механізмів виявлення вторгнень та наведені переваги їх використання.

Також детально проаналізовано системи запобігання вторгнень, які працюють на основі правил та аномалій.

В якості прикладу було використано Microsoft ATA та центр безпеки Azure, що був використаний в якості гібридного рішення для поведінкового аналізу користувачів комп'ютерної мережі.

На основі розглянутої концепції виявлення та запобігання вторгнень можливо побудувати ефективну систему сповіщення за захисту мереж.

Рис. 12. Сповіщення від Deep Security Agent

Список літератури

1. Широчин В. П., Мухін В. Є., Кулик А. В. Питання проектування засобів захисту інформації в комп'ютерних системах та мережах. Київ; «СТОЛІТТЯ+». 2000. – 111 с.
2. Ганієв С. К., Карімов М. М. «Питання оптимального сегментування топології локальних комп'ютерних мереж».-Ташкент, Проблеми інформатики та енергетики, 2001 № 2.-С.20-25.
3. Stephen Northcutt, Judy Novak. Network Intrusion Detection: An Analysts Handbook Third Edition,2001. – 384 p.
4. Michael Collins. Network Security Through Data Analysis: From Data to Action 2nd Edition, 2017. – 428 p.
5. Yuri Diogenes, Erdal Ozkaya. Cybersecurity – Attack and Defense Strategies, 2020. – 326 p.

Received (Надійшла) 10.03.2022
Accepted for publication (Прийнята до друку) 11.05.2022

Concept of the system of detection and prevention of networks

O. Makarenko, A. Yanko

Abstract. Detecting and preventing network attacks is one of the most important tasks of a network security system. It is now difficult to find a network that does not have such active attack prevention tools as antivirus, firewall, intrusion prevention and detection systems. Unfortunately, active means of repelling attacks alone are not enough. Therefore, in addition, passive means of combating attacks are used - network intrusion detection systems. Therefore, this article is devoted to protecting computer networks from attacks, intrusions and unauthorized access. Particular attention is paid to the principle of operation of network systems for detection and prevention of intrusions. This article discusses the different types of intrusion detection mechanisms and the benefits of their use. Intrusion prevention systems that operate on the basis of rules and anomalies are also analyzed in detail. Behavioral analytics of UEBA users and objects for detection of security breaches are considered. As an example, we used Microsoft ATA and Azure Security Center, which was used as a hybrid solution for behavioral analysis of computer network users. The example of the Azure Security Center explores intelligent security tools and the expansion of analytics to more quickly detect threats and reduce the number of false alarms. Based on the considered concept of detection and prevention of intrusions, it is possible to build an effective notification system for network protection.

Keywords: active network sensor, information security, computer network, network intrusion detection systems, unauthorized access, intrusion prevention system.