ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ НА БАЗІ FORTIGATE IPS»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Павловський О. Ю.
(прізвище та ініціали)
Керівник Власенко В. О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

ЦОД – центр обробки даних

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

DMZ – Demilitarized Zone

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPS – Intrusion Prevention System

IPsec – IP security

NGFW – Next Generation Firewall

NGIPS – Next Generation Intrusion Prevention Systems

SOC – Security Operation Center

SIEM – Security Information and Event Management

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Розвиток корпоративних мережевих інфраструктур призвів до розширення поверхні атаки для відомих, невідомих та загроз нульового дня.

Оскільки першопричини більшості порушень пов'язані з використанням відомих вразливостей, багато організацій, щоб не відставати, звернулися до систем запобігання вторгнень (IPS). Правильна IPS пропонує найбільш ефективний спосіб блокувати загрози, які використовують відомі вразливості.

Запобігання вторгнень включає не тільки глибоку перевірку пакетів, яка вивчає те, що знаходиться всередині трафіку, але також забезпечує інші аспекти, такі як зіставлення зі зразком, виявлення аномалій і інші потреби, які повинні виконуватися на швидкості передачі даних, з прийняттям рішень за мікросекунди щоб заблокувати або дозволити трафік.

IPS можна застосувати як автономну IPS або ж цю функцію втілюють в консолідовані функції IPS всередині міжмережевого екрану наступного покоління (NGFW). IPS використовує сигнатури, які можуть застосовуватися для виявлення вразливостей, так і експлуатуватись специфічно для ідентифікації шкідливого трафіку. Зазвичай це виявлення на основі сигнатури або виявлення на основі статистичної аномалії для виявлення шкідливої діяльності.

Виявлення на основі сигнатур використовує однозначно ідентифікувані сигнатури, які містяться в коді експлойту. Коли виявляються рухи, їх сигнатури потрапляють у базу даних, яка все більше розширюється. Виявлення сигнатур на основі IPS включає або сигнатури, спрямовані на експлуатацію, які ідентифікують самі експлойти, або сигнатури, що стикаються з вразливістю, які визначають вразливість системи, на яку спрямовано атаку. Сигнатури, що стикаються з вразливістю, важливі для виявлення потенційних варіантів експлуатації, які раніше не спостерігались, але вони також збільшують ризик помилково позитивних результатів (доброякісні пакети, помилково позначені як загрози).

Статистичне виявлення на основі аномалії випадково відбирає мережевий трафік, а потім порівнює вибірки з базовими рівнями продуктивності. Коли зразки виявляються поза межами базової лінії, IPS запускає дію, щоб запобігти потенційній атаці.

Тому, від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки корпоративної мережі.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження методів та засобів виявлення та попередження вторгнень в корпоративну мережу.

Об'єкт дослідження – захист корпоративної мережі.

Предмет дослідження – технологія виявлення та попередження вторгнень в корпоративну мережу.

Мета роботи – розробити порядок застосування технології виявлення та попередження вторгнень в корпоративну мережу та рекомендації щодо його реалізації.

Наукові завдання:

проаналізувати проблему захисту корпоративної мережі;

визначити зміст проблеми виявлення та попередження вторгнень в корпоративну мережу;

дослідити існуючі методи та засоби виявлення та попередження вторгнень в корпоративну мережу;

розглянути порядок втілення та застосування системи виявлення та попередження вторгнень в корпоративну мережу;

розробити рекомендації щодо виявлення та попередження вторгнень в корпоративних мережах.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці

рекомендацій щодо виявлення та попередження вторгнень в корпоративні мережі.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференція «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2021 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ВИЯВЛЕННЯ ТА ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ

1.1. Аналіз проблеми захисту корпоративних мереж

В [2] наводиться такий приклад, що на початку 2020 року велика організація охорони здоров'я державного сектора США зіткнулася з серйозним витоком даних, що зачіпає більше 1,1 мільярда медичних записів одержувачів допомоги. На жаль, кількість кібератак проти державного сектора США зростає. Фактично, Cybersecurity Ventures повідомляє, що державний сектор США в даний час входить в п'ятірку найбільш схильних до кібератак бізнес-секторів в світі.

Наведемо деякі цифри. Глобальні кібератаки за минулий рік [2]:

4 трильйони спроб кібер вторгнень;

10 мільярдів кібератак зловмисного програмного забезпечення;

187 мільйонів кібератак вимагачів;

34 мільйони кібератак Інтернету речей (IoT).

Статистика та факти уряду США та кіберзлочинності [5]:

США найбільше постраждали від кіберзлочинності з точки зору фінансових збитків;

у 2019 році федеральний уряд США зіткнувся із збитками на суму понад 13,7 млрд. дол. США в результаті кібератак;

відсутність достатнього бюджету кібербезпеки є головною перешкодою для ефективної кіберпрограми на рівні штату в США.

За даними IBM [4], вартість витоку кіберданих у всьому світі становить 3,9 мільйона доларів, середня вартість витоку кіберданих у США становить 8,2 мільйона доларів.

Розглянемо топ десять тенденцій кібербезпеки в США [2]:

1. Збільшення витрат на кібербезпеку державними установами: у 2021 році передбачається, що федеральні, штатні та місцеві державні видатки США на кібербезпеку збільшаться на 5% або більше, включаючи витрати на дослідження та

розробки (НДДКР), обладнання, програмне забезпечення, професійні послуги – освіта в галузі кібербезпеки, тренінги, моделювання, розвідка кіберзагроз, управління вразливістю, послуги центру безпеки, кіберінженерія, служби реагування на інциденти – та індивідуальні інтегровані рішення з кібербезпеки. Очікуване збільшення інвестицій у кібербезпеку необхідне для боротьби зі зростанням кіберзагроз, націлених на урядові установи США.

2. Зростання кібератак на урядові установи США: державний сектор США повинен збільшити кількість та рівень витонченості таких типів кібератак: phishing, brute-force, distributed denial of service (DDoS), trojan horse malware, business email compromise (BEC), advanced persistent threat (APT) malware.

3. Змішування акторів кіберзагроз, націлених на урядові установи США: передбачається подальше поєднання акторів кіберзагроз, включаючи кібератаку національних держав групи (Китай, Росія, Іран, Північна Корея та інші), злочинні кібератаки та хактивісти, що працюють разом і націлені на федеральні, державні та місцеві урядові установи США. Зокрема, передбачається, що кібератаки на урядові установи США викрадають інтелектуальну власність, отримують особисту інформацію ключових урядових та військових керівників, проводять кампанії дезінформації та затримують/порушують критичні державні операції.

4. Потенційний зрив моделі монетизації викупних програм: у жовтні 2020 року Управління контролю за іноземними активами Міністерства фінансів США (OFAC) попередило компанії та державні та місцеві урядові установи, які здійснюють платежі за викуп, що вони ризикують порушити економічні санкції, введені федеральним урядом США проти кіберзлочинного угрупування або кібератаки, що фінансуються національною державою. Різко зменшивши виплати за допомогою кібервикупу, OFAC має потенціал порушити поточну модель монетизації викупних програм і, в кінцевому рахунку, призвести до зменшення кількості кібератак з вимогами в цілому по країні, що було б дуже позитивно для державного сектору США.

5. Необхідність вдосконалення безпечного доступу до віддаленої віртуальної приватної мережі (VPN): в результаті пандемії COVID-19 протягом 2021 року

будуть продовжуватись потребувати посилених заходів з кібербезпеки для підтримки надзвичайного зростання віддаленого доступу за допомогою VPN, необхідних для державних службовців , державні підрядники та онлайн-діяльність між громадянами

6. Зростання хмарної інфраструктури та додатків вимагає більшої кібербезпеки: передбачається, що федеральні, штатні та місцеві урядові установи США збільшать міграцію хмар із центрів обробки даних у загальнодоступні хмари (тобто AWS, Microsoft, IBM та інші) та приватні хмари. що вимагатиме посилених заходів інформаційної безпеки для поліпшення кібергігієни та забезпечення конфіденційності даних, захисту даних та їх стійкості.

7. Посилення інсайдерських загроз: оскільки рівень обізнаності щодо кібербезпеки зростає, а операції з кіберзахисту посилюються федеральними, штатними та місцевими урядовими установами США, очікується зростання кіберінсайдерських загроз. Актори кіберзагрози (особливо групи кібератак національних держав) добре відомі тим, що пристосовують свою кібер-тактику, техніку та процедури (ТТП) до ситуації, завжди шукаючи найслабшу ланку для проведення нападу. Таким чином, у міру вдосконалення освіти, тренінгів, обладнання та програмного забезпечення в урядових установах США, учасники кіберзагроз намагатимуться підкупити, погрожувати та/або шантажувати інсайдерів державних установ, щоб отримати доступ до цінної національної оборонної інформації, викрасти інтелектуальну власність або незаконно отримати особисту інформацію для впливу на керівників уряду. *За даними Verizon Security, у 2020 році понад 35% усіх порушень кіберданих були прямим результатом інсайдерських загроз.*

8. Зростання цифрової трансформації зумовлює збільшення кіберзахищеності: оскільки федеральні, державні та місцеві урядові установи США впроваджуватимуть численні проекти цифрової трансформації із застосуванням нових технологій штучного інтелекту, машинного навчання, аналізу великих даних, мобільних технологій 5G, Інтернет речей (IoT), підключені пристрої. Ці технології, орієнтовані на дані, можуть створити набагато більше вразливих місць

інформаційної безпеки, якщо тільки попередні заходи з кібербезпеки не будуть заплановані та прийняті в авангарді проектів.

9. Висока текучість американських фахівців з кібербезпеки: згідно з доповіддю Gartner Group за 2020 рік, лише в США є понад 4 мільйони незаповнених вакансій у інформаційних технологій (IT) та у галузі кібербезпеки, багато з цих відкритих посад у кібербезпеці потрібно швидко заповнити. Як результат, у 2021 р ймовірно буде тривати високий коефіцієнт обігу 20% і більше досвідчених фахівців у галузі кібербезпеки, від аналітиків безпеки середнього рівня до головних службовців інформаційної безпеки (CISO) по всій країні.

10. Еволюція регуляторного ландшафту в галузі кібербезпеки: передбачається, що федеральні, штатні та місцеві урядові установи США продовжуватимуть намагатися йти в ногу з новими технологіями та постійно змінювати кіберзагрози. Таким чином, передбачається, що США приймуть нові закони, нормативні акти, стандарти та сертифікації з питань кібербезпеки, щоб спробувати стримати зростання кібератак як у державному, так і в приватному секторах, вимагаючи посилення програм управління ризиками кібербезпеки, посиленого моніторингу, виявлення та можливості реагування на інциденти та покарання за недбалість щодо інформаційної безпеки

У 2021 році федеральні, державні та місцеві урядові установи США повинні інвестувати мільярди доларів платників податків у рішеннях з кібербезпеки для зменшення кібер-ризиків та боротьби з кібератаками. Крім того, очікується, що урядові установи США впровадять численні багатомільярдні програми цифрової трансформації, використовуючи нові технології: хмарні обчислення, аналіз великих даних, автоматизацію даних, AI, ML та автоматизацію роботизованих процесів з метою вдосконалення державних послуг, збільшити швидкість аналізу даних, покращити процес прийняття рішень та зменшити експлуатаційні витрати.

Вищезазначені інформаційні технології, що виникають, відкривають потенціал для значних рішень, орієнтованих на дані, для різних оперативних завдань уряду. Подібно до цього кожна з цих технологій створює нові ризики кібербезпеки та кіберзахист до потенційних порушень даних, що може поставити

під загрозу конфіденційність даних та безпеку даних для державних службовців та всіх громадян США.

Розуміння ландшафту атак може допомогти групам безпеки пріоритезувати ресурси, вивчити найбільш ймовірні сценарії і виявити зміни в методах зловмисників. Головні тенденції атак, виявлених IBM Security X-Force [6] в 2020 році: програми-вимагачі, безсумнівно, є основним типом атак, за якими слід крадіжка даних і атаки доступу до сервера. З точки зору початкових векторів атак сканування і експлойт піднялися на перше місце в 2020 році, за ним послідували фішинг і крадіжка облікових даних.

Top 3 attack types	**Top 3 initial attack vectors**
1. Ransomware (23% of attacks)	1. Scan-and-exploit (35% of attacks vs. 30% in 2019)
2. Data theft (160% increase since 2019)	2. Phishing (33% of attacks vs. 31% in 2019)
3. Server access (233% increase since 2019)	3. Credential theft (18% of attacks vs. 29% in 2019)

Рис. 1.1. Головні тенденції атак, виявлених в 2020 році IBM Security X-Force [6]

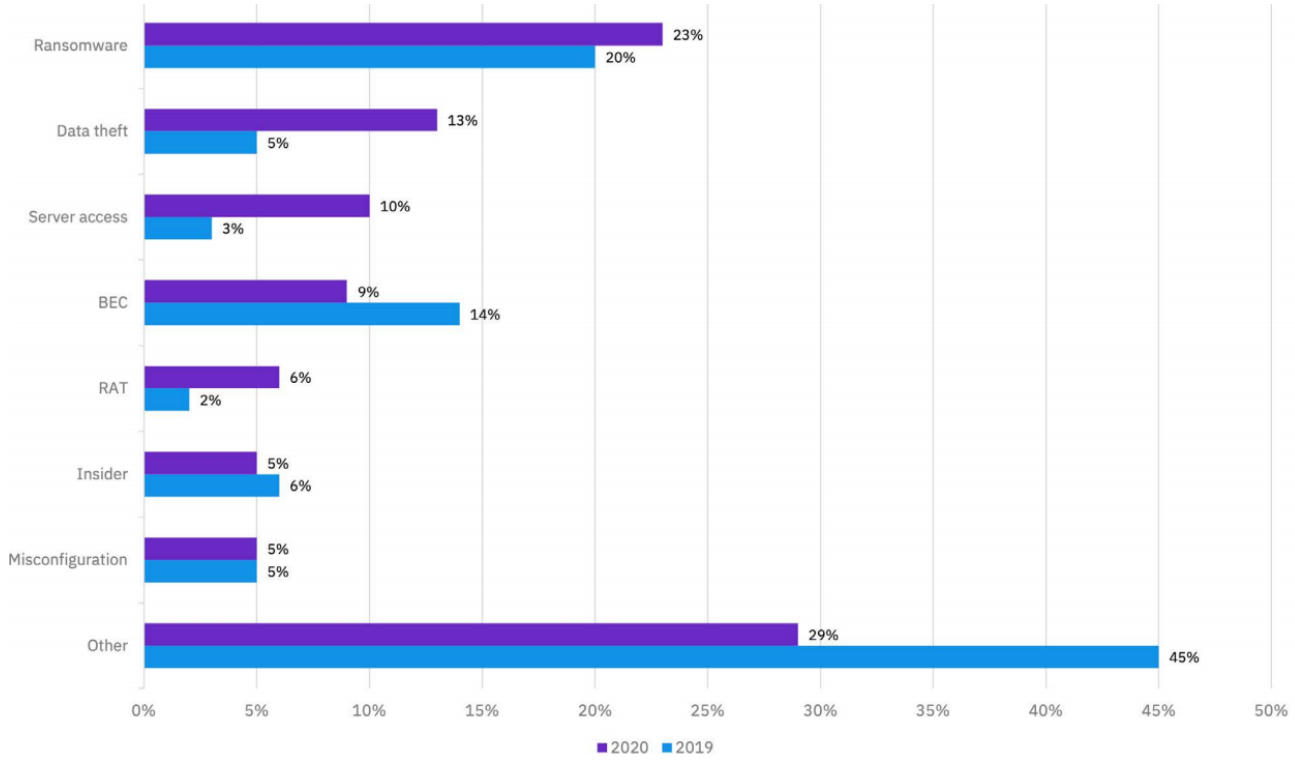

Рис. 1.2. Топ типів кібератак у порівнянні 2019/2020 роки за даними IBM Security X-Force [6]

За даними FortiGuard Labs [7], зловмисники переміщують значні ресурси для націлювання і використання нових периферійних мережевих середовищ, таких як віддалені співробітники і хмара. За останні кілька років мережі радикально змінилися. Простіше кажучи, традиційний периметр мережі був замінений декількома периферійними середовищами: локальна мережа (LAN), глобальна мережа (WAN), мультіхмара, центр обробки даних, віддалений працівник, Інтернет речей (IoT), пристрої мобільного зв'язку і багато іншого – кожне зі своїми унікальними ризиками і вразливостями.

Одним з найбільш значних переваг для кіберзлочинців в усьому цьому є те, що, хоча всі ці межі взаємопов'язані, часто через те, що додатки і робочі процеси переміщаються між декількома середовищами або між ними, багато організацій пожертвували централізованою видимістю і уніфікованим контролем на користь продуктивності і гнучкості.

Забезпечення безпеки нових середовищ, включаючи нові технології і конвергентні системи, є більш складним завданням, ніж може здатися. Наприклад, перехід до віддаленої роботи – це не тільки збільшення числа кінцевих користувачів і пристроїв, віддалено підключаються до мережі [7].

Додавання просунутого штучного інтелекту дозволить кіберзлочинцям навчитися виявляти і долати захисні стратегії. Крім того, очікується збільшення кількості скомпрометованих мереж периферійних пристроїв, які продаються як послуга. Ці шкідливі прикордонні мережі потім можуть використовуватися для обробки інформації, збору інформації про цілі або запуску скоординованої атаки, яка одночасно націлена на максимальну кількість векторів атаки, тим самим пригнічуючи захист [7].

Використання великих скомпрометованих мереж (в основному периферійних) пристроїв може дозволити просунутим кіберзлочинцям наблизитися до обчислювальної потужності корпоративних мереж. І як тільки ця проблема буде вирішена, поява таких ресурсів у вигляді служби даркнета стане лише питанням часу. Це означає, що організації, які відстають у впровадженні та розвитку систем на основі штучного інтелекту і передових методів з безпеки, з

великою ймовірністю, ніж будь-коли, зіткнуться з такою тактикою [7].

При використанні кіберзлочинцями роїв на основі ботів можуть використовуватися для швидкого подолання мережевого захисту, ефективного пошуку і вилучення критично важливих даних, а також видалення або компрометації криміналістичної інформації [7].

1.2. Призначення, принцип роботи та основні функції систем виявлення вторгнень

У більшості SOC система виявлення інцидентів і збору даних по ним спирається на набір мережевих сенсорів, розміщених в інфраструктурі замовника. Для здійснення якісного моніторингу мережі аналітику необхідні три елементи [1]:

початкове спрацьовування сигнатурної або поведінкової системи виявлення вторгнень (IDS). Сюди ж входить можливість використання для користувача сигнатур і доступ до інформації про продукт тієї сигнатури або поведінки, який спрацював (наприклад, синтаксис сигнатури);

дані NetFlow, що відображають зведення зі взаємодії вузлів, перерахованих в спрацьовуванні, за кілька днів або тижнів до і після спрацювання;

захоплення пакетів, які спровокували спрацьовування, бажано повної сесії в форматі libpcap (PCAP).

При наявності цих трьох елементів, ефективної аналітики та робочих процесів, аналітик може виявити аномальну або зловмисну активність і визначити, які необхідні подальші дії. В ідеалі, спрацьовування IDS і події NetFlow необхідно зіставляти з даними PCAP для полегшення роботи аналітика. Однак деякі рішення добре справляються з усіма трьома завданнями, тому SOC доводиться комбінувати кілька продуктів. Згідно кращим практикам, SOC необхідно доповнити ці три пасивні системи вбудованими превентивними засобами типу NIPS або засобами детонації контенту.

Системи виявлення вторгнень (IDS), згідно з визначенням у [1], це апаратні або програмні засоби, які збирають і аналізують дані комп'ютерної системи або мережі з метою виявлення потенційних порушень системи безпеки, до яких

відносяться як зовнішні атаки, так і внутрішні інциденти (зловживання).

Відштовхуючись від цього визначення, мережеві IDS – це IDS, які захоплюють і аналізують мережевий трафік на предмет потенціальних вторгнень і інших підозрілих або несанкціонованої активності.

IDS зіставляє трафік в режимі реального часу з політиками сигнатур, визначенням прийнятної/нормальної поведінки і набором інших евристик, генеруючи оповіщення, які надсилаються на консоль і в базу даних.

Кожен раз, коли IDS вловлює підозрілу активність, наприклад, за випадковим збігом з однією з сигнатур, вона генерує попередження. Це попередження має містити повний опис, щоб аналітик SOC зміг зрозуміти, як його інтерпретувати і що робити. Типове попередження від IDS (особливо, від мережевої сигнатурної IDS) складається з наступних полів [1]:

ID події;

дата і час (іноді з точністю до мілісекунд) спрацьовування сигнатури;

IP джерела і призначення;

UDP або TCP порт джерела і призначення;

назва або ID сигнатури;

критичність події;

текстовий опис сигнатури або посилання на зовнішній репозиторій або базу даних з детальною інформацією по сигнатурі, наприклад, на запис CVE і опис сигнатури;

відправлені та отримані байти для всієї мережевої сесії, під час якого відбулося спрацьовування;

додаткова контекстна інформація, що включає по можливості поля, специфічні для конкретного протокола- SNMP, SMTP, POP3, HTTP, FTP, SSL або CIFS/SMB.

Попередження від IDS іноді також включають посилання на вихідний PCAP пакета(ів), на яких спрацювала сигнатура або на сесію цілком. Замість того, щоб включати всі ці дані в кожне попередження, можна додати в опис події посилання, щоб аналітик міг отримати PCAP дані при необхідності.

NIDS можуть бути як в апаратної (у вигляді пристрою), так і в програмній формі. Вони можуть використовувати сигнатурні або поведінкові методи, як ми сказали раніше, і навіть в певних випадках їх комбінувати. NIDS можуть також діяти в просторі між атакуючим і його жертвою, не просто повідомляючи про шкідливої активності, а й активно її блокуючи. Такі системи називаються NIPS – мережевими системами запобігання вторгнень [1].

Великі SOC зазвичай розміщують кілька NIPS або NIDS сенсорів в основних вузлових точках – в точках периметра мережі, підключення до Інтернету, іноді ключових світчей і маршрутизаторів. NIDS виконує команди центру управління, наприклад, по оновленню сигнатур, і відправляє назад Попередження, які генерують детективні модулі. Аналітик може увійти в центр управління через веб-консоль, переглянути статуси сповіщень і системи, управляти політиками сенсорів. Ця архітектура представлена на рис. 1.3.

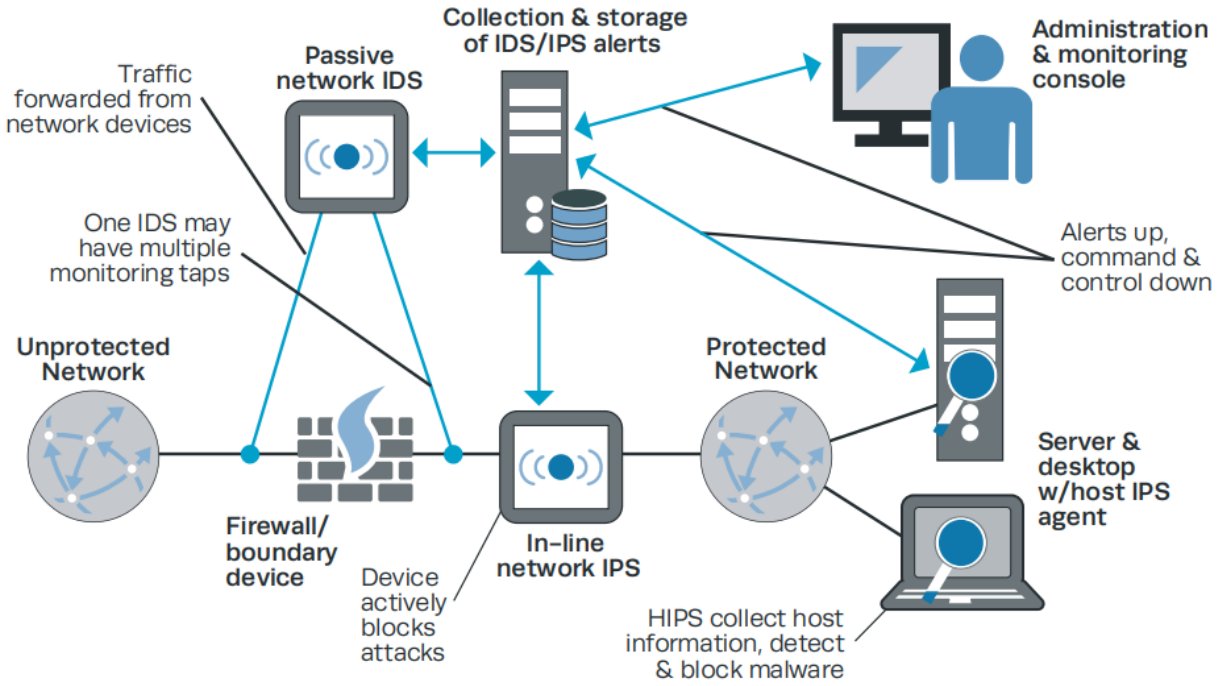

Рис. 1.3. Типова архітектура IDS/IPS [1]

Універсальні IDS, які здійснюють моніторинг всіх протоколів в рівній мірі, часом на шкоду більш детальному аналізу конкретного типу трафіку. Такі системи становлять більшість засобів виявлення і запобігання, які використовуються множиною зрілих SOC, однак вони не закривають всі прогалини. Тому їх можна

доповнити засобами виявлення і запобігання, специфічними для конкретного протоколу і часом розмиваючими кордони між IDS/IPS і MCE. Подібні рішення спеціалізуються на одному протоколі, наприклад, XML, на SQL-трафіку, веб-трафіку або трафіку веб-служб. Зазвичай в них реалізовані надійні механізми захоплення і аналізу трафіку для виявлення і блокування шкідливої активності, що не детектується універсальними системами виявлення. Такі рішення добре застосовувати для обслуговування критичних сервісів, які використовує величезна маса користувачів.

У кожній з різних типів систем виявлення є свої переваги і недоліки. Вони наведені в таблиці 1.1.

Для сучасних фахівців із захисту мереж ймовірно найважливіша функція IDS – детектувати ті атаки, від яких організація повноцінно не захищена. С моменту виявлення атаки до установки на системи патчів або розгортання інших захисних заходів. І цей факт підкреслює важливість поведінкових IDS, що не залежать від сигнатур і своєчасного оновлення бази сигнатур IDS.

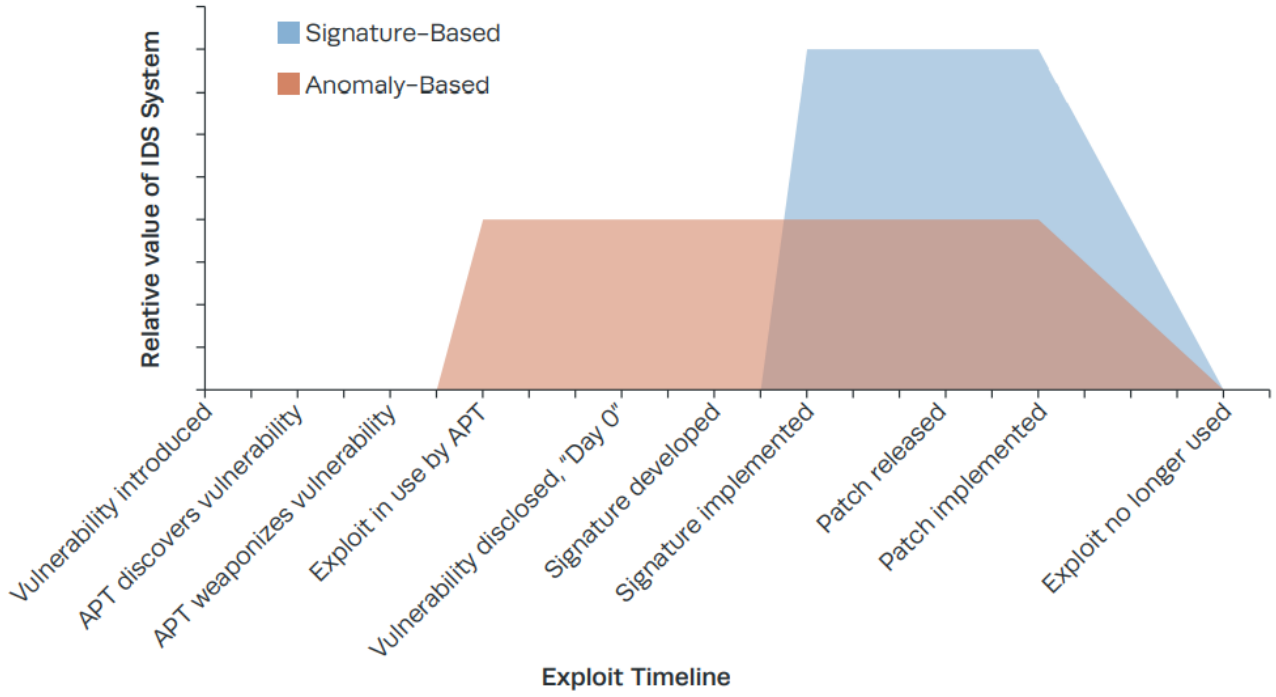

Рис. 1.4. Порівняння відносної цінності системи виявлення і життєвого циклу сигнатури [1]

Таблиця 1.1

Порівняння різних типів систем виявлення

Характеристика	Тип	Переваги	Недоліки
Метод виявлення	Поведінковий: відомий як виявлення аномалій	Поведінкові IDS можуть виявляти раніше не виявлені атаки і несанкціоноване використання в рамках сесії ще до того, як про атаку стало широко відомо (так звані атаки нульового дня). Вони складні і схильні до помилкових спрацьовувань.	Вони вимагають більше часу на навчання системи стандартам прийнятної поведінки. Мережі або системи, схильні до частих оновлень і стрибків активності, може бути складно змоделювати для забезпечення ефективного моніторингу.
	Інтелектуальний: відомий як виявлення по сигнатурам або виявлення несанкціонованого використання	Виявлення, засноване на сигнатурах, дає швидкий результат і менший рівень помилкових спрацьовувань, ніж поведінковий виявлення. Сигнатурні IDS можуть миттєво виявляти відомі атаки.	Сигнатурні IDS можуть виявляти лише відомі атаки. Якщо сигнатури не оновлюється, IDS буде пропускати нові типи атак, в результаті, атакуючі і захисники будуть грати в кішки-мишки. Схильні до помилкових спрацьовувань. Їх можна обдурити шляхом спотворення контенту або шифрування протоколу.
Джерело	Мережеві: виявляють активність в мережевому трафіку на периметрі або ключових точках моніторингу	Мережеві IDS можуть відстежувати широкий діапазон систем кожним з розміщених сенсорів. Повинні бути невидимі користувачам.	Мережеві IDS можуть пропускати трафік і схильні до спуфінгу, атакам і обходу. Мережеві IDS часто не можуть виявити, чи була атака успішної чи ні. Мережеві IDS не можуть перевірити зашифрований трафік.
	Хостові (локальні): забезпечують моніторинг	Хостові IDS (HIDS) вловлюють трафік атакуючого, спрямований на систему, навіть якщо мережевий	Вмілий хакер може заблокувати або обійти програми хостових IDS. Налаштування хостової IDS досить

	операційної системи і призначеної для користувача активності. Сенсорами служать програмні агенти, які розміщуються в використовуваних системах.	трафік відсутня, зашифрований або спотворений, оскільки HIDS його детектує за активністю системи або логам. Хостова IDS може допомогти оцінити успіх або провал атаки. Хостова IDS може допомогти у виявленні несанкціонованого використання легітимним користувачем. Хостова IDS часто володіє додатковими можливостями, наприклад, з відстеження цілісності/ довіреності хостів.	трудомістке, оскільки багато хто з них використовують механізми виявлення, які легко обійти, або ж вимагають нетривіального навчання (і перенавчання) нормальної поведінки систем. Хостова IDS часто вимагає привілейованих прав доступу до систем для запобігання або блокування несанкціонованого використання. Неправильно настроєна хостова IDS може перешкоджати коректній роботі хоста.
Режим реагування	Активний: Активні IDS, звані IPS, реагують шляхом припинення сервісу або блокування виявлених активностей противника.	IPS добре комбінувати з сигнатурними IDS в силу потреби в добре відомих визначеннях атак. IPS можуть запобігати або знижувати збиток за рахунок швидкого реагування на загрозу або атаку. Не вимагають миттєвого втручання оператора.	IPS вимагають деякого контролю над сервісами, які вони моніторять. IPS вимагають ретельної настройки для того, щоб уникнути блокування або зниження продуктивності легітимного трафіку або активності вузла.
	Пасивний: Пасивні IDS реагують шляхом розсилки попереджень або алертів. Вони не здійснюють ніяких коригувальних заходів.	Легше розгорнути. Помилкові спрацьовування не мають негативного впливу на системи замовника.	Все попередження вимагають втручання оператора. Це вимагає додаткового часу на інтерпретацію, підбір відповідних дій і реагування, що може привести до більшого збитку.

Як видно з рис. 1.4, система виявлення надає найбільшу цінність з моменту впровадження експлойта атакуючим до установки патчів проти нього. Можна також зауважити, що сигнатурним системам виявлення притаманне відставання з моменту розміщення експлойта до розробки сигнатури. Оскільки сигнатурні системи виявлення зазвичай точніше детектують атаку, після установки відповідної сигнатури така система може вважатися більш ефективною стосовно даного експлойту, ніж працює на евристиці. У міру зменшення використання експлойта цінність такої системи виявлення щодо конкретної вразливості також знижується.

Пасивні системи виявлення надають SOC необхідні дані і спрацьовування, проте нічого не запобігають, просто формують необхідний набір даних, який використовується іншими інструментами і аналітиками. Якщо ми зможемо скористатися технологіями, які дозволять блокувати атаки в режимі реального часу, це дасть більший результат [1].

Мережеві IPS мають такі можливості, однак вимагають ще більшої пильності і тонкої настройки, оскільки потенційно можуть впливати на роботу мережі і доступність.

Щоб ефективно скористатися можливостями NIPS, SOC важливо врахувати деякі моменти, пов'язані з їх використанням. До них відносяться [1]:

помилкові спрацьовування. З огляду на високий рівень помилкових спрацьовувань, властивий системам виявлення, адміністратори NIPS небезпідставно гранично обережні. Уявімо, що кожне помилкове спрацьовування буде приводити до блокування трафіку. Якщо адміністратор NIPS буде необережний, його дії призведуть до серйозної відмови в обслуговуванні. В результаті, багато SOC дуже ретельно відбирають сигнатури NIPS, які будуть приводити до блокувань і тільки після декількох днів або тижнів тестування в режимі тільки виявлення. Тому вкрай важливо вибрати NIPS з надійним аналізом протоколів і механізмом сигнатурного виявлення;

варіанти реакції у відповідь. Різні технології IPS пропонують різні варіанти реакції на шкідливий трафік. Один з методів полягає в скиданні TCP на обох вузлах,

що беруть участь в з'єднанні, однак, це не дуже вдала ідея. Атакуючий ймовірно очікує таку реакцію, тому далі він: 1) може просто ігнорувати скидання і продовжувати з'єднання; 2) тепер уже знає, що має справу з IPS, яку потрібно обійти. Деякі IPS здійснюють блокування за рахунок автоматичного оновлення списку управління доступом міжмережевого екрану або маршрутизатора, блокуючи підозрілу мережеву взаємодію. Це теж проблемний варіант, оскільки призводить до хаосу в конфігураціях міжмережевого екрану і маршрутизаторів. Правильні IPS здійснюють блокування самостійно – просто скидаючи шкідливі пакети і всі наступні між вузлами атакуючого і жертви;

відповідні дії. Давайте розглянемо такий приклад, коли IPS блокує пакети в ході зловмисного з'єднання і не здійснює ніяких інших дій, наприклад, скидання TCP. Скільки за часом слід забороняти взаємодія атакуючого і з ким – тільки з жертвою або взагалі з усіма? Архітектурні особливості мережі, наприклад, використання NAT, можуть це ускладнити. Уявімо IPS, яка засікла атаку, як би йде від веб-проксі або міжмережевий екран з NAT. IPS може прийняти міжмережевий екран за атакуючого, хоча насправді це взагалі інший вузол ззовні. Але оскільки ми блокуємо трафік, ми скидаємо пакети на власному міжмережевому екрані, тим самим викликаючи відмову в обслуговуванні (DoS). Для коректних дій у відповідь дуже важливо вкрай акуратно розміщувати IPS;

присутність. NIPS не повинна розкривати свою присутність ніяким іншим системам. Це означає, що вона не повинна відправляти трафік ні атакуючому, ні жертві і мати MAC-адресу. Іншими словами, пристрій повинен сприйматися як «перешкода з'єднання». При цьому навіть найкраща IPS може розкрити свою присутність, просто виконуючи свою роботу. Умілий атакуючий може засікти вбудовану NIPS, використовуючи старі методики атак. Вони майже напевно не приведуть до успіху, тому що проти них вже поставлені поновлення. Однак NIPS буде продовжувати свою роботу з блокування атакуючого від будь-яких подальших з'єднань. В результаті атакуючий зрозуміє, що зіткнувся з NIPS і може змінити тактику нападу. Тому SOC може віддати перевагу вибірковому блокуванню атак, а не повною заборони всіх атакуючих IP;

час очікування і пропускна здатність. Перебуваючи в центрі мережевого трафіку, NIPS може надавати небажаний вплив на працездатність мережі. Погано реалізована або неправильно підібрана NIPS може викликати затримки в мережевих з'єднаннях, ненавмисно знижувати пропускну здатність або гальмувати трафік, якій проходить через неї. Щоб уникнути цієї проблеми, SOC повинен обережно підходити до вибору NIPS для роботи з конкретними мережевими з'єднаннями, особливо, високошвидкісними;

вартість аналізу трафіку. NIPS може працювати на заявленої швидкості тільки з певним набором протоколів або з відключенням певних модулів аналізу. Наприклад, NIPS розрахована на 10 гігабіт, може працювати на 2 гігабіта з увімкненим модулем аналізу HTTP-трафіку через ресурсоємності HTTP і логіки, необхідної для детектування атак з цього протоколу. Або ж NIPS може заявляти про підтримку відкритого формату сигнатур (наприклад, Snort), але використання цієї можливості істотно знизить швидкість обробки трафіку механізму виявлення NIPS. Крім цього багато NIPS можуть надавати функції міжмережевого екранування і шейпінгу трафіку. Використання цього функціоналу з великою ймовірністю призведе до зниження продуктивності оброблюваного мережевого трафіку. Фахівцям SOC необхідно ретельно оцінити, чи надасть воно істотний вплив на мережеві сервіси;

модифікація контенту. Деякі з інструментів IPS, особливо, ті, які заявляють про наявність можливостей щодо припинення промислового шпигунства і витоків даних, можуть не тільки блокувати трафік, але і за фактом його модифікувати. Сюди може входити видалення частини даних з веб-сторінок або документів Word в процесі переміщення по мережі. Це дуже складне завдання, тому що вимагає відтворення сесії протоколу і модифікації на ще більш високому рівні абстракції, ніж мережевий трафік. Наприклад, розглянемо додаток, яке очікує певну кількість байт, і це значення вказано в полі протоколу як контрольна сума. Якщо переданий контент модифікований, контрольна сума повинна бути перерахована. Чи може IDS це здійснити, не провокуючи істотних затримок в мережевому трафіку? Такі технології досить складні і рекомендуються до використання тільки в SOC, добре

забезпечених ресурсами;

єдина точка збою. Якщо IPS встановлена «в розрив», що відбудеться в разі її поломки або відключення? Гарна IPS має можливості (або доповненнями), які дозволяють їй залишатися у відкритому стані при відмові (тобто в разі збою і відключення живлення, вона продовжить пропускати трафік). Це може здаватися невдалою ідеєю, але пам'ятайте про те, що IPS – не єдиний засіб захисту мережі від зовнішнього світу. Поблизу повинні бути маршрутизатори та міжмережеві екрани, які налаштовуються на правила відмови за замовчуванням. Більшість комерційних вендорів NIPS вбудовують можливості відкритого збою, тому потрібно передбачити запобіжні заходи або архітектурні зміни при розміщенні відкритої IPS на типовому обладнанні;

участь в мережевих операціях. Коли SOC розміщує будь-які інструменти «в розрив» де-небудь в організації (HIPS, NIPS або щось ще), вони де факто стають учасниками мережевих операцій. Найчастіше будь-які інструменти SOC звинувачують в тому, що викликають проблеми різного характеру (збої мережі або низьку продуктивність), навіть якщо зв'язок між обладнанням і реальними проблемами надумана. SOC слід чітко контролювати статус пристроїв і потоків даних для своєчасного виявлення проблем та постійно працювати з командою мережевих операцій для гарантії того, що обладнання поводиться належним чином;

вартість. NIPS не терпить низьку продуктивність або доступність, як пасивна IDS. Тому вендорам NIPS доводитися вбудовувати надійне, часом втілювати обладнання в свої продукти. Стандартний сенсор NIDS може коштувати менше $ 10 тис., При цьому NIPS, що працює на тих же швидкостях, може коштувати значно дорожче. Більшість NIDS на поточному ринку мають подвійну функцію: вони можуть працювати як пасивно осторонь, так і активно «в розрив». Проте робота «в розрив» вимагає в два рази більше портів на пристрої, що подвоює ефективну вартість роботи «в розрив» для певного набору мережевих каналів.

Незважаючи на ці труднощі, деякі SOC вважають NIPS вельми корисним інструментом. Часовий проміжок між розробкою експлойта і установкою патча є період підвищеного ризику для компанії; іноді він становить кілька годин, а іноді

кілька тижнів або місяців. Кілька грамотно розміщених IPS дадуть той необхідний рівень захищеності в періоди, коли системи замовника особливо уразливі [1].

На жаль, багато SOC ніколи не переводять свої NIPS в блокуючий режим. За результатами спілкування з кількома SOC і розробниками IPS, деякі, якщо не більшість, пристроїв залишаються в пасивному режимі налагодження/виявлення протягом практично всього періоду експлуатації.

Потенційних причин для цього декілька [1]:

1) у SOC немає необхідних організаційних повноважень і операційної маневреності;

2) у SOC немає достатньої впевненості в налаштуваннях своїх сигнатур;

3) SOC просто вважає, що ризики, що виникають у зв'язку з переведенням в блокуючий режим «на розрив», не виправдовують можливий ризик спровокувати DoS.

Звичайно, існують і інші методи вбудованого блокування атак, які вважають за краще використовувати замість NIPS деякі SOC – пристрої детонації контенту і хостової IPS [1].

1.3. Аналіз існуючих методів та засобів щодо попередження вторгнень в корпоративну мережу

IDPS в першу чергу орієнтовані на виявлення можливих інцидентів. Наприклад, IDPS може виявити, коли зловмисник успішно скомпрометував систему, скориставшись уразливістю в системі. Потім IDPS може повідомити про інцидент адміністраторам безпеки, які можуть швидко ініціювати дії з реагування на інцидент, щоб мінімізувати збиток, заподіяний інцидентом [3].

IDPS може також реєструвати інформацію, яка може бути використана аналітиками інцидентів. Багато IDPS також можна налаштувати для розпізнавання порушень політик безпеки. Наприклад, деякі IDPS можуть бути налаштовані з настройками, аналогічними набору правил брандмауера, що дозволяє їм визначати мережевий трафік, який порушує політику безпеки або допустимого використання організації [3].

Крім того, деякі IDPS можуть відслідковувати передачу файлів і виявляти підозрілі, наприклад копіювання великої бази даних на портативний комп'ютер користувача. Багато IDPS також можуть ідентифікувати розвідувальну діяльність, яка може вказувати на неминучість атаки. Наприклад, деякі інструменти атак і шкідливі програми, зокрема хробаки, виконують розвідувальні операції, такі як сканування хостів і портів, для визначення цілей для подальших атак. IDPS може бути в змозі заблокувати розвідку і повідомити адміністраторів безпеки, які можуть вдатися до дій, якщо необхідно, змінити інші заходи безпеки для запобігання пов'язаних інцидентів. Оскільки в Інтернеті так часто ведеться розвідка, виявлення рекогносцировки часто виконується в першу чергу в захищених внутрішніх мережах [3].

Крім виявлення інцидентів і підтримки зусиль з реагування на інциденти, організації знайшли інші застосування для IDPS, включаючи наступне [3]:

виявлення проблем безпекової політики. IDPS може забезпечити певний рівень контролю якості для реалізації політики безпеки, наприклад, дублювання наборів правил брандмауера і попередження, коли він бачить мережевий трафік, який повинен був бути заблокований брандмауером, але не через помилки конфігурації брандмауера;

документування існуючої загрози для організації. IDPS реєструють інформацію про виявлені ними загрози. Розуміння частоти і характеристик атак на обчислювальні ресурси організації допомагає визначити відповідні заходи безпеки для захисту ресурсів. Інформацію також можна використовувати для інформування керівництва про загрози, з якими стикається організація;

утримання людей від порушення політик безпеки. Якщо люди знають, що їх дії відстежуються технологіями IDPS на предмет порушень політики безпеки, вони з меншою ймовірністю здійснять такі порушення через ризик виявлення.

Через зростаючої залежності від інформаційних систем, а також з-за поширеності і потенційного впливу вторгнень на ці системи IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації.

Розглянемо *ключові функції технологій IDPS*. Існує багато типів технологій

IDPS, які розрізняються в першу чергу типами подій, які вони можуть розпізнати, і методологіями, які вони використовують для ідентифікації інцидентів.

Крім моніторингу та аналізу подій для виявлення небажаної активності, всі типи технологій IDPS зазвичай виконують такі функції [3]:

запис інформації, що відноситься до спостережуваних подій. Інформація зазвичай записується локально, а також може бути відправлена в окремі системи, такі як сервери централізованої реєстрації, рішення для управління інформацією і подіями (SIEM) і системи управління підприємством;

повідомлення адміністраторів безпеки про важливі спостережувані події. Це повідомлення, відоме як попередження, відбувається за допомогою будь-якого з декількох методів, включаючи наступні: електронні листи, сторінки, повідомлення в призначеному для користувача інтерфейсі IDPS, пастки протоколу SNMP, повідомлення системного журналу, а також призначені для користувача програми і сценарії. Такі повідомлення зазвичай включають в себе тільки основну інформацію про подію; адміністраторам необхідно отримати доступ до IDPS для отримання додаткової інформації;

складання звітів. Звіти узагальнюють відслідковують події або надають детальну інформацію про конкретні події, що представляють інтерес. Деякі IDPS також можуть змінювати свій профіль безпеки при виявленні нової загрози. Наприклад, IDPS може збирати більш детальну інформацію для конкретного сеансу після виявлення шкідливої активності в цьому сеансі. IDPS може також змінити налаштування, коли спрацьовують певні попередження або який пріоритет слід призначати наступним попередженням після виявлення конкретної загрози.

Виявлення вторгнень – це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі, і їх аналізу на наявність ознак можливих інцидентів, які представляють собою порушення або неминучі загрози порушення політик комп'ютерної безпеки, політик допустимого використання або стандартних методів забезпечення безпеки [3].

Запобігання вторгнень – це процес виявлення вторгнень і спроби зупинити виявлені можливі інциденти. Системи виявлення й запобігання вторгнень (IDPS) в

першу чергу орієнтовані на виявлення можливих інцидентів, реєстрацію інформації про них, спроби їх зупинити і повідомлення про них адміністраторам безпеки. Крім того, організації використовують IDPS для інших цілей, таких як виявлення проблем з політиками безпеки, документування існуючих загроз і утримання людей від порушення політик безпеки. IDPS стали необхідним доповненням до інфраструктури безпеки майже кожної організації [3].

Існує багато типів технологій IDPS, які розрізняються в першу чергу типами подій, які вони можуть розпізнати, і методологіями, які вони використовують для виявлення можливих інцидентів. У даній публікації обговорюються наступні чотири типи технологій IDPS [3]:

на основі мережі, яка відстежує мережевий трафік для певних сегментів мережі або пристроїв і аналізує активність протоколу мережі і додатків для виявлення підозрілої активності;

в безпроводовій мережі, яка відстежує і аналізує трафік безпроводової мережі для виявлення підозрілої активності, пов'язаної з самими протоколами безпроводової мережі;

аналіз мережевої поведінки (NBA), який досліджує мережевий трафік для виявлення загроз, які створюють незвичайні потоки трафіку, таких як DDoS-атаки, сканування і певні форми шкідливого ПЗ;

на основі хоста, який відстежує характеристики окремого хоста і події, що відбуваються всередині цього хоста, на предмет підозрілої активності.

IDPS зазвичай записують інформацію, що відноситься до спостережуваних подій, повідомляють адміністраторів безпеки про важливі спостережувані події і створюють звіти.

Багато IDPS також можуть реагувати на виявлену загрозу, намагаючись запобігти її успішне виконання. Вони використовують кілька методів реагування, які включають в себе зупинку атаки IDPS, зміна середовища безпеки (наприклад, перенастроювання брандмауера) або зміна вмісту атаки.

IDPS не можуть забезпечити повністю точне виявлення; всі вони генерують помилкові спрацьовування (неправильне визначення доброякісної діяльності як

шкідливої) і помилково негативні (нездатність ідентифікувати шкідливу активність). Багато організацій вважають за краще налаштовувати IDPS таким чином, щоб кількість помилкових спрацьовувань зменшувалася, а кількість помилкових спрацьовувань збільшувалася, що вимагає додаткових ресурсів аналізу, щоб відрізняти помилкові спрацьовування від справжніх шкідливих подій [3].

Більшість IDPS також пропонують функції, які компенсують використання звичайних методів ухилення, які змінюють формат або час шкідливої активності, щоб змінити її зовнішній вигляд, але не її ефект, щоб спробувати уникнути виявлення IDPS.

Більшість IDPS використовують кілька методологій виявлення, окремо або разом, щоб забезпечити більш широке і точне виявлення. Основні класи методів виявлення наступні [3]:

на основі сигнатури, яка порівнює відомі сигнатури загроз з подіями, які спостерігаються, для виявлення інцидентів.

Це дуже ефективно при виявленні відомих загроз, але в значній мірі неефективно при виявленні невідомих загроз і багатьох варіантів відомих загроз. Виявлення на основі сигнатур не може відстежувати і розуміти стан складних комунікацій, тому воно не може виявити більшість атак, що складаються з декількох подій;

виявлення на основі аномалій, яке порівнює визначення того, яка діяльність вважається нормальною, з подіями, які спостерігаються, для виявлення значних відхилень. У цьому методі використовуються профілі, розроблені шляхом відстеження характеристик типової активності протягом певного періоду часу. Потім IDPS порівнює характеристики поточної активності з граничними значеннями, пов'язаними з профілем.

Методи виявлення на основі аномалій можуть бути дуже ефективними при виявленні раніше невідомих загроз. Загальні проблеми з виявленням на основі аномалій включають ненавмисне включення зловмисних дій в профіль, створення профілів, які недостатньо складні для відображення реальної обчислювальної

активності, і створення безлічі помилкових спрацьовувань;

аналіз протоколу з відстеженням стану, який порівнює заздалегідь певні профілі загальноприйнятих визначень доброякісної активності протоколу для кожного стану протоколу з спостерігаються подіями для виявлення відхилень.

На відміну від виявлення на основі аномалій, яке використовує профілі, що залежать від хоста або мережі, аналіз протоколів з відстеженням стану спирається на розроблені постачальником універсальні профілі, які визначають, як конкретні протоколи повинні і не повинні використовуватися.

Він здатний розуміти і відслідковувати стан протоколів, що мають поняття стану, що дозволяє йому виявляти багато атак, які інші методи не можуть. Проблеми з аналізом протоколів з відстеженням стану включають в себе те, що часто дуже складно або неможливо розробити повністю точні моделі протоколів, це дуже ресурсномістке і не може виявляти атаки, які не порушують характеристики загальноприйнятої поведінки протоколу.

По можливості, організаціям слід розглянути можливість використання мереж управління для розгортання мережевих IDPS. Якщо IDPS розгорнуто без окремої мережі управління, організації повинні подумати про те, чи потрібна VLAN для захисту комунікацій IDPS [3].

Крім вибору відповідної мережі для компонентів, адміністраторам також необхідно вирішити, де повинні бути розташовані датчики IDPS. Датчики можуть бути розгорнуті в одному з двох режимів [3]:

вбудований датчик розгорнуто так, що мережевий трафік, який він відстежує, повинен проходити через нього, так само як потік трафіку, пов'язаний з фаєрволом. Фактично, деякі вбудовані датчики являють собою гібридні пристрої брандмауера/IDPS, а інші – просто пристрої IDPS.

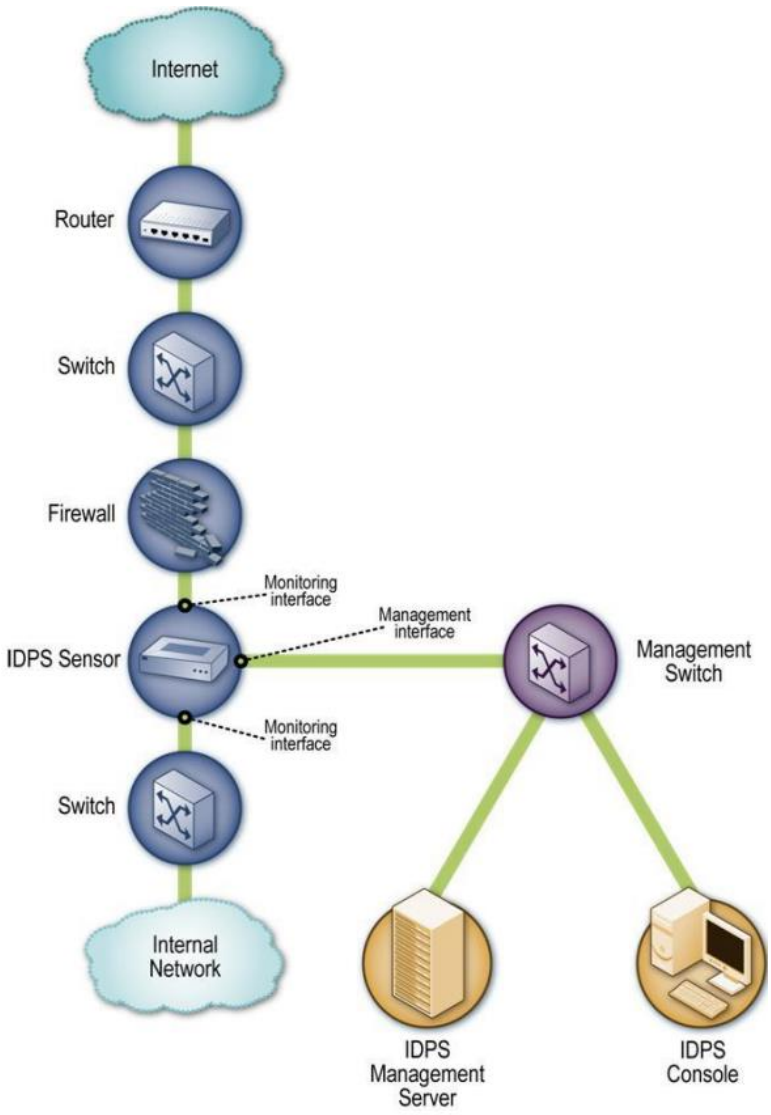

Рис. 1.5. Приклад вбудованої мережевої архітектури датчиків IDPS [3]

Основна мотивація для розгортання вбудованих датчиків IDPS – дати їм можливість зупинити атаки, заблокувавши мережевий трафік. Вбудовані датчики зазвичай розміщуються там, де повинні бути розміщені мережеві брандмауери та інші пристрої мережевої безпеки - на розділах між мережами, таких як сполуки з зовнішніми мережами і кордони між різними внутрішніми мережами, які слід розділити. Вбудовані датчики, які не є гібридними пристроями брандмауера/IDPS, часто розгортаються на більш захищеній стороні мережеві, щоб у них було менше трафіку для обробки. На рис. 1.5 показано таке розгортання. Датчики також можуть бути розміщені на менш захищеній стороні мережі, щоб забезпечити захист і знизити навантаження на міжмережевий екран.

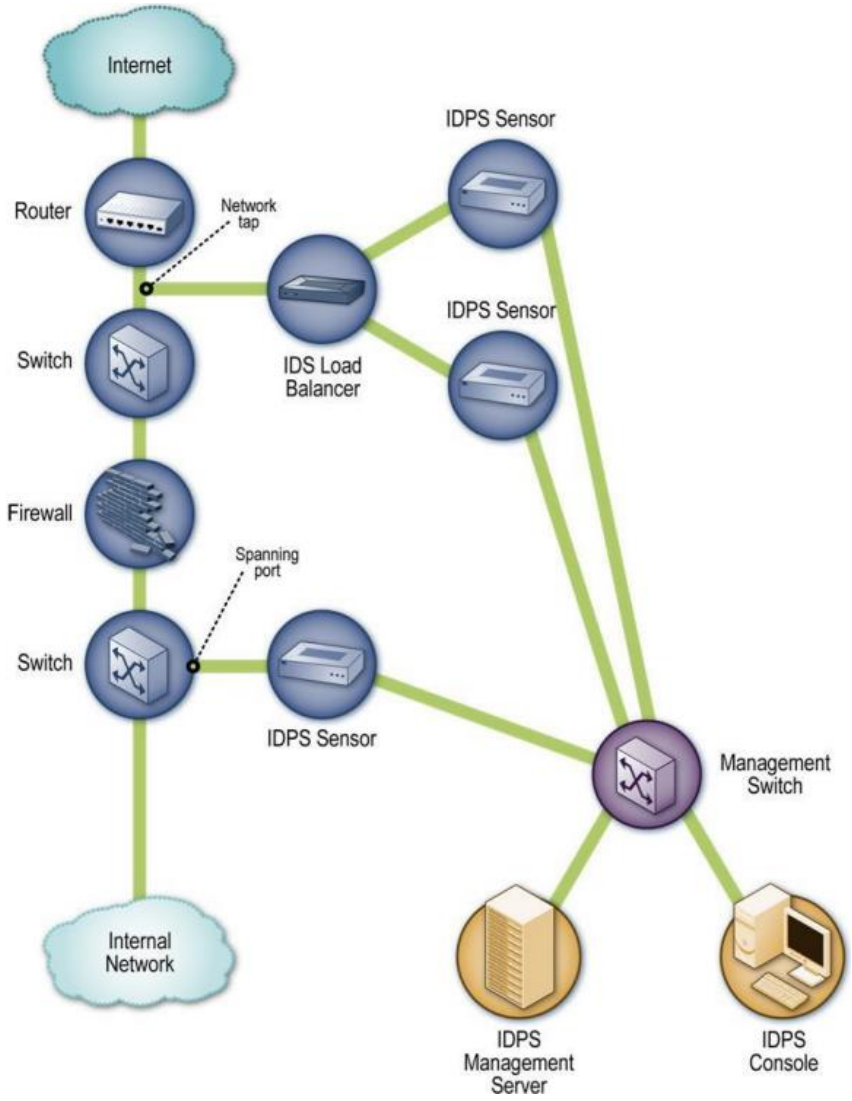

Рис. 1.6. Приклад архітектури пасивного мережевого датчика IDPS [3]

пасивний. Розгорнуто пасивний датчик, який відстежує копію фактичного мережевого трафіку (рис. 1.6). Насправді трафік через датчик не проходить. Пасивні датчики зазвичай розгортаються так, щоб вони могли контролювати ключові місця розташування в мережі, такі як поділ між мережами, і ключові сегменти мережі, такі як активність в підмережі демілітаризованої зони (DMZ).

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ НА БАЗІ РІШЕННЯ FortiGate IPS

2.1. Підхід до попередження вторгнень в корпоративну мережу

Технологія запобігання вторгнень (IPS) все ширше застосовується в системах мережевої безпеки. Вона доступна як в форматі одного з компонентів мережевого доступу, так і у вигляді окремого автономного засобу.

Компанія Fortinet, одним з найвідоміших продуктів якої є міжмережевий екран наступного покоління (NGFW), більше десяти років займалася розробкою технології IPS. Клієнти Fortinet звикли покладатися на високу продуктивність міжмережевих екранів FortiGate. Рішення FortiGate IPS розроблено на основі кращої на ринку технології IPS і повністю виправдовує свою вартість і очікування клієнтів.

Розробка рішення FortiGate IPS ведеться в напрямку, відмінному від розвитку традиційних технологій IPS, тому ми маємо можливість впроваджувати інноваційні функції, які не підтримуються іншими автономними рішеннями IPS.

Загрози «нульового дня», просунуті цілеспрямовані атаки, програми-вимагачі, поліморфне шкідливе ПЗ і розподілені атаки типу «відмова в обслуговуванні» вимагають складних механізмів виявлення, які відсутні в традиційних автономних системах IPS і в більшості міжмережевих екранів.

Рішення FortiGate IPS включає в себе кілька комплексних модулів перевірки, джерел даних про загрози і варіантів захисту від просунутих загроз для захисту від невідомих загроз. FortiGate IPS – це потужне рішення на декількох платформах FortiGate (апаратні, віртуальні, хмарні засоби) з функцією поглибленого аналізу та управління робочими процесами через компонент FortiAnalyzer, яке представляє собою економічно ефективне рішення для забезпечення безпеки мережі, що відповідає вимогам реагування на інциденти в центрі управління системою безпеки (SOC) організації.

Система запобігання проникненню (IPS) є найважливішим компонентом основних можливостей безпеки кожної мережі. Він захищає від відомих загроз та атак нульового дня, включаючи шкідливе програмне забезпечення та основні вразливості.

Процесори безпеки FortiGate забезпечують безпрецедентну високу продуктивність, тоді як FortiGuard Labs інформує провідні в галузі аналітичні дані про загрози, що створює перевірений успіх у захисті від відомих загроз. Як ключовий компонент Fortinet Security Fabric, FortiGate IPS захищає всю наскрізну інфраструктуру без шкоди для продуктивності.

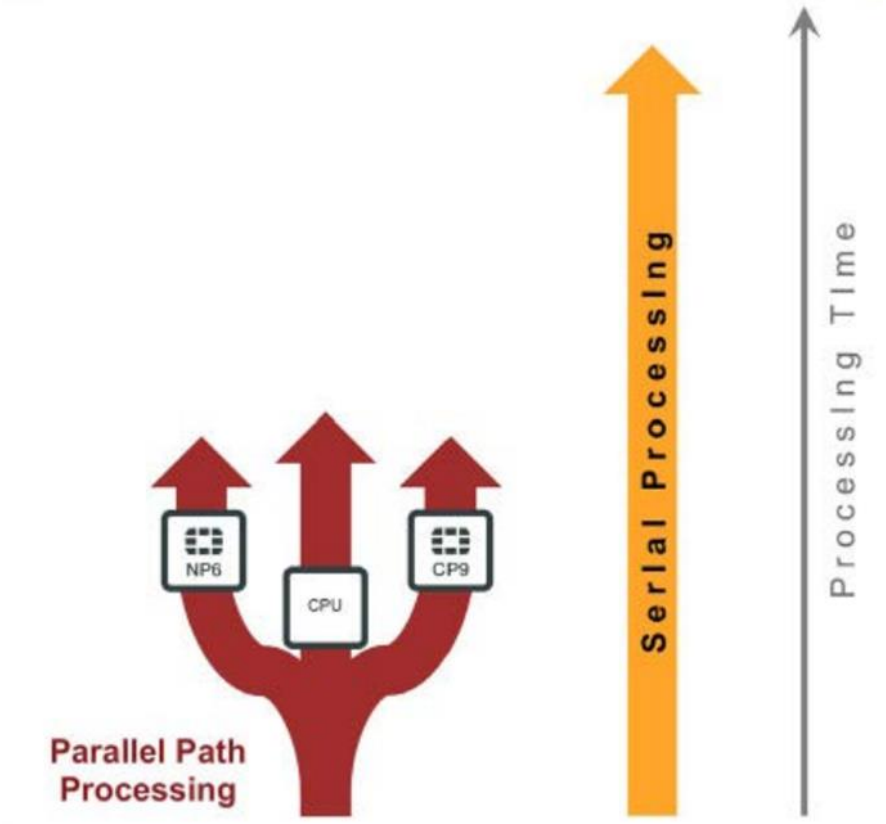

Рис. 2.1. Апаратний базис FortiGate

Ландшафт загроз продовжує розвиватися, і поверхня атаки для всіх організацій розширюється. Оскільки першопричини більшості порушень пов'язані з використанням відомих вразливостей, багато організацій, щоб не відставати, звернулися до систем запобігання вторгнень (IPS). Правильна IPS пропонує найбільш ефективний спосіб блокувати загрози, які використовують відомі вразливості. Fortinet FortiGate надає кращі в своєму класі можливості IPS для мережевої інфраструктури, заснованої на безпеці, забезпечуючи тонкий баланс та

високу ефективність безпеки без порушення бізнес-процесів. FortiGate IPS побудований на унікальній архітектурі спеціалізованих процесорів безпеки і мережевих процесорів (рис. 2.1), які дозволяють йому забезпечувати безпрецедентну продуктивність в поєднанні з FortiGuard Labs – дослідницькою групою з аналізу загроз [11].

Розширення поверхні атаки в поєднанні з мінливим ландшафтом загроз призвело до того, що підприємства розгортають всі доступні інструменти безпеки для захисту від новітніх загроз. Такий підхід до реалізації точкового підходу привів до вибухового зростання кількості інструментів безпеки і постачальників, розгорнутих всередині організації [11].

В середньому типова група безпеки великого підприємства використовує понад 50 різних інструментів безпеки від декількох поставщіков. Але такий підхід призводить до величезних додаткових витрат і викликає безліч проблем: від відсутності автоматизації та інтеграції до сліпих зон в загальній видимості IT-інфраструктури [11].

Традиційно підприємства розгортали автономну систему IPS, щоб підвищити рівень безпеки, перевіряючи трафік на наявність загроз. Основною причиною впровадження автономної IPS була нездатність традиційних корпоративних міжмережевих екранів забезпечити високу ефективність захисту від загроз при високій продуктивності без впливу на затримку в мережі [11].

Інша важлива причина полягала у відсутності гнучкості і можливості налаштувуватися при захисті від загроз, що часто було недоліком міжмережевих екранів другого покоління [11].

Отже, багато організацій, які відчувають нестачу кваліфікованого персоналу в своїх групах безпеки, знаходяться в розпалі ініціатив щодо забезпечення безпеки, що прагнуть замінити застарілі системи IPS, щоб випереджати просунуті загрози в мережевому ландшафті. Організаціям необхідне рішення щодо забезпечення безпеки, яке пропонує значні поліпшення з точки зору спрощення операцій по забезпеченню безпеки і завдань управління, підвищення ефективності безпеки, а також кращої видимості і контролю їх мережі. Інтеграція IPS з технологією

мережевого доступу нового покоління (NGFW) ефективно вирішує вищезазначені проблеми, дозволяючи організаціям вийти за рамки традиційної IPS і запровадити інтегрований, набагато більш ефективний підхід до мережевої безпеки [11].

Запобігання вторгнень включає не тільки глибоку перевірку пакетів, яка вивчає те, що знаходиться всередині трафіку, але також забезпечує інші аспекти, такі як зіставлення зі зразком, виявлення аномалій і інші потреби, які повинні виконуватися на швидкості передачі даних, з прийняттям рішень за мікросекунди щоб заблокувати або дозволити трафік [11].

У NGFW FortiGate використовуються спеціалізовані процесори безпеки, звані «процесори контенту», які дозволяють FortiGate переносити ресурсомісткі завдання, такі як IPS, на виділені процесори, що практично не впливає на продуктивність. FortiGate при розгортанні як NGFW з вбудованою функцією IPS забезпечує високу пропускну здатність з низькою затримкою для захисту центру обробки даних і базової мережі підприємства [11].

Висока ефективність безпеки з аналізом загроз FortiGuard Labs – це глобальна організація Fortinet, що займається аналізом загроз і дослідженнями. Його місія – надавати клієнтам найкращу в галузі інформацію про загрози, щоб захистити їх від зловмисних кібератак. Використовуючи мільйони глобальних мережевих датчиків, FortiGuard Labs відстежує поверхню атак по всьому світу і використовує штучний інтелект (AI) для пошуку цих даних на предмет нових загроз [11].

Зусилля великий глобальної команди досвідчених мисливців за загрозами, дослідників, аналітиків, розробників інструментів і фахівців з обробки даних дозволяють FortiGuard Labs підтримувати всі продукти Fortinet в актуальному стані, надаючи найкращу доступну інформацію про ідентифікацію загроз та захисту [11].

На сьогоднішній день виявлено більше 860 вразливостей нульового дня, і FortiGuard Labs створює поновлення аналітики загроз для продуктів безпеки Fortinet, щоб забезпечити їх новітній захист від загроз. Сюди входять поновлення аналітики загроз для міжмережевих екранів і IPS наступного покоління Fortinet, а також рішення для захисту від вірусів, спаму, пісочниці, кінцевих точок і

електронної пошти. У відповідних випадках це також включає поновлення репутації шкідливих URL-адрес, IP-адрес і доменів [11].

Коли справа доходить до мережевої безпеки, розрізнені продукти зазвичай не можуть обмінюватися даними про загрози або координувати заходи в рамках інфраструктури організації. Ця критична нестача кібербезпеки часто ускладнюється браком кваліфікованого персоналу служби безпеки для управління широким асортиментом відключених точкових продуктів. Але навіть у великих організаціях зі спеціалізованим персоналом по IT-безпеки все ще виникають труднощі з моніторингом мережі, щоб відстежувати, які пристрої підключені, у кого є доступ до мережі і які ресурси необхідні для яких додатків і робочих процесів [11].

Рішення для централізованого управління з єдиною панеллю, таке як Fortinet Fabric Management Center, забезпечує оптимізовану видимість, знижує складність. Це дозволяє групам безпеки і експлуатації мережі відслідковувати переміщення даних і виявляти аномальну активність, спрощує оптимізацію рішення і централізує управління функціями безпеки, такими як управління політиками і елементами, для всього розгортання. Групи безпеки можуть створювати політику в єдиній точці, яка потім може бути розподілена по всій IT-інфраструктурі, будь то локальний центр обробки даних або приватні і загальнодоступні хмари. Дане рішення також спрощує операції для адміністраторів і співробітників з обмеженими ресурсами, вимагаючи менше людино-годин при одночасному зниженні сукупної вартості володіння (TCO).

Таким чином, *коли справа доходить до захисту від відомих вразливостей і вразливостей нульового дня, системи запобігання вторгнень грають вирішальну роль в силу їх здатності використовувати такі функції, як віртуальне виправлення, щоб забезпечити більш швидкий час захисту.* Як в автономному IPS, так і в конвергентному розгортанні NGFW інноваційна система FortiGate IPS забезпечує перевірений захист світового класу. Як частина Fortinet Security Fabric, FortiGate IPS використовує глобальну і локальну аналітичну інформацію про безпеку з іншими рішеннями Fortinet і довіреними сторонніми продуктами, забезпечуючи

оцінку ризиків з використанням найактуальнішої інформації, а також поліпшення загального стану безпеки [11].

Критики автономних систем запобігання вторгнень (IPS) заявляють, що ринок сповільнюється або навіть скорочується, вважаючи, що це причина для пошуку альтернатив технології IPS. У той час як багато автономні продукти IPS в невеликих філіях і кампусах середнього розміру замінюються технологією IPS, об'єднаної в брандмауер, триваюче розвиток центрів обробки даних привело до вибухового зростання автономних розгортання IPS [14].

Незалежно від того, чи є вона частиною брандмауера або окремим автономним пристроєм, технологія IPS стає все більш поширеною частиною засобів захисту мережевої безпеки. Жодна організація, стурбована витонченими і цільовими атаками, не може дозволити собі ігнорувати захист, який забезпечується глибокою перевіркою IPS. Однак така глибока перевірка IPS стає дорогої з точки зору обчислень через постійно зростаючого обсягу трафіку центру обробки даних, змушуючи організації балансувати свої агресивні вимоги до продуктивності з реальністю консервативних бюджетів. Більш того, навіть якщо проблеми з продуктивністю вирішені, нестача талантів в кваліфікованих фахівцях з безпеки змушує команди до такої міри, що робоче навантаження перевищує їх можливості [14].

Основні характеристики і переваги FortiGate IPS [14]:

глибока перевірка на наявність складних загроз, ботнетів, нульових днів і цільових атак в мережі;

незалежна стороння перевірка демонструє чудову виявлення і краще співвідношення ціни і якості;

інноваційна технологія процесора безпеки (SPU) для високопродуктивної мережевої пропускної здатності і ретельної перевірки безпеки;

повна інтеграція – пристрій або хмарна служба – з ізольованим програмним середовищем світового класу для розширених загроз;

спеціальні заходи безпеки для веб-серверів і додатків, включаючи міжсайтовий сценарії і SQL-ін'єкції;

засоби захисту даних для запобігання крадіжки конфіденційних даних.

FortiGate IPS є просунутим та відповідає високим стандартам повної IPS наступного покоління (NGIPS).

2.2. Призначення та можливості рішення FortiGate IPS

Системи запобігання вторгнень (IPS) відіграють ключову роль в захисті корпоративної мережі і центру обробки даних, перевіряючи трафік в пошуках шкідливого контенту [12].

Системи IPS були розроблені для доповнення мережевого брандмауера. На самому базовому рівні брандмауери фільтрують мережевий трафік на основі визначених правил, блокуючи вхід для трафіку, який явно не схвалений. Пристрої IPS спроектовані так, щоб розташовуватися після брандмауера і перед внутрішньою мережею, перевіряючи зв'язок і аналізуючи шаблони трафіку в реальному часі для виявлення і запобігання атак. Вони служать додатковим рівнем захисту для підвищення рівня безпеки компанії і часто потрібні на відповідність вимогам [12].

Але оскільки перевірки IPS вимагають великих ресурсів і занадто багато з них можуть вплинути на продуктивність мережі, важливо, щоб брандмауер спочатку відсікав трафік, який не можна пропускати в мережу. Він порівнює вхідний трафік з певними правилами, забезпечуючи доступ тільки явно дозволеним повідомленнями. Він перевіряє, звідки прийшов трафік, хто його відправив або метод транспортування (тип програми). *Але, строго кажучи, це не стосується корисного навантаження* [12].

Пристрій IPS перевіряє корисне навантаження, щоб переконатися, що в мережу не потрапляють шкідливі програми або атаки під виглядом легітимного трафіку. Брандмауери орієнтовані на джерело трафіку, відправника трафіку і тип програми, що передає трафік. Після того як брандмауер відповів на ці питання, він ігнорує баланс пакетів в потоці. Навпаки, пристрої IPS повинні перевіряти корисне навантаження в кожному пакеті потоку, щоб переконатися у відсутності шкідливого вмісту. Компанії досягають найвищого рівня безпеки в своїй мережі

або в своєму центрі обробки даних, коли вони одночасно використовують обидва ці підходи до перевірки [12].

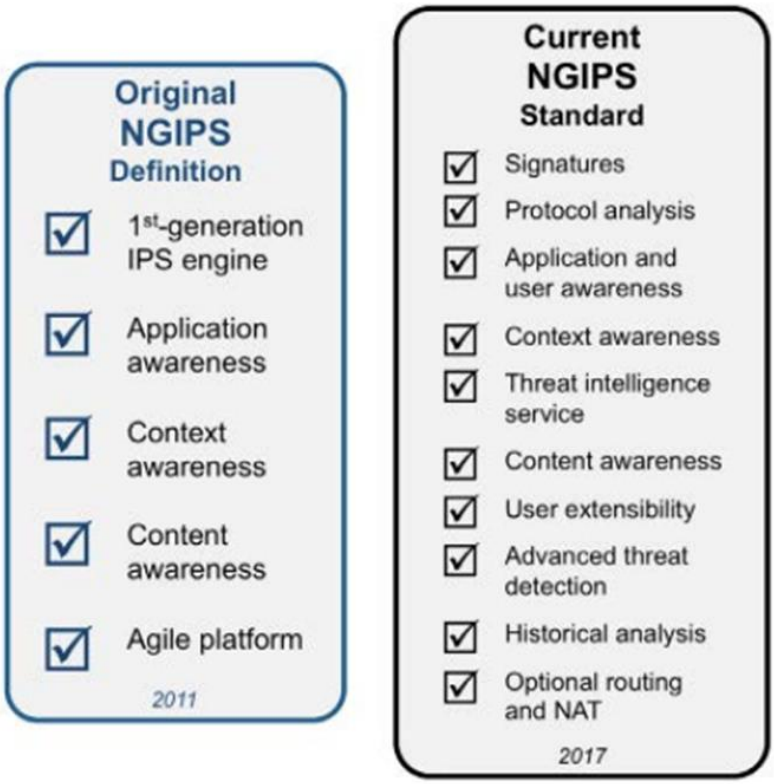

Рис. 2.2. Розвиток можливостей NGIPS [12]

Перше покоління систем IPS (рис. 2.2) було зосереджено на виявленні сигнатур, порівнюючи вхідні пакети з сигнатурами відомих загроз. Цей підхід дозволив відобразити безліч спроб атак, але в міру розвитку загроз він залишив пролом в корпоративній безпеці: будь-яка атака, яка не має розпізнаної сигнатури, пройшла б через IPS. Згодом стало ясно, що одне тільки виявлення сигнатур не може адекватно захистити від множинних векторів атак цільових загроз і поліморфізму [12].

IPS розвиваються у міру зміни ландшафту загроз. Системи IPS нового покоління вийшли за рамки зосередження виключно на виявленні сигнатур. Їх процеси перевірки пакетів включають обізнаність про контекст, інформацію про зміст, а також обізнаність про додатки і користувачів. Автономні пристрої IPS нового покоління також пропонують розширене виявлення загроз і пов'язані з авторитетними службами аналізу загроз [12].

Включення всієї цієї інформації в аналіз загроз IPS дозволяє краще приймати

рішення про те, які пакети дозволити пропускати, і дає їм змогу краще виявляти атаки нульового дня, складні загрози і бот-мережі. У той же час з'явилися NGFW. *NGFW включають в себе IPS і інші типи функцій безпеки, які компаніям, що мають тільки міжмережевий екран першого покоління, доводилося розгортати і керувати ними окремо.* Однак, додавання цих функцій в NGFW не завжди ідеально [12].

Різні постачальники систем IPS використовують різні підходи до вирішення проблем та можливостей сучасного ринку. Деякі постачальники відреагували продажем технологій IPS. Інші зробили придбання, щоб розширити свою продуктову лінійку. *Крім того, є виробники, такі як IBM, які вирішили покинути ринок IPS. У серпні 2017 року компанія оголосила, що припинить продаж продуктової лінійки IBM Network Security (XGS) в кінці того ж года*. IBM продовжить підтримувати поточних клієнтів до 2022 року, але ці клієнти не зможуть додавати пристрої, тому що IBM більше не продає XGS. Це означає, що клієнти можуть продовжувати зберігати статус-кво, але вони не можуть розширювати свої системи IPS, та поліпшень або оновлень не буде. Таким чином, для багатьох клієнтів IBM має сенс дуже скоро почати пошуки заміни [12].

Гарна новина полягає в тому, що у компаній є два шляхи для просування захисту IPS: вони можуть встановити як автономну IPS, так і брандмауер, або вони можуть розгорнути NGFW, який може виконувати обидві функції [12].

Варіант 1: автономна IPS. Для великих кампусів і центрів обробки даних, для яких безпека додатків і даних має першорядне значення, потрібна перевірка контенту, яка є в IPS наступного покоління, яка зазвичай доступна тільки в автономних пристроях IPS. За оцінками NSS Labs, ринок впровадження автономних пристроїв IPS в центрах обробки даних, зокрема (ринок DCIPS), оцінюється в 450 мільйонів доларів США в рік, і прогнозує сукупний річний темп зростання цього ринку на рівні 15% до 2020 року [12].

Для підприємств зі складними мережами, великими центрами обробки даних або особливо гостро стурбованих безпекою додатків або даних слід серйозно подумати про встановлення автономної IPS на додаток до міжмережевого екрану.

Фактично, компанії, яким потрібна максимальна продуктивність і безпеку для свого центру обробки даних або корпоративної мережі, часто вважають за краще розгортати міжмережевий екран NGFW і автономний NGIPS. Можливості запобігання вторгнень в автономній IPS часто більш надійні, ніж в більшості NGFW. Навіть зараз багато NGFW включають технологію IPS, яка по суті все ще є механізмом зіставлення сигнатур [12].

Вони перевіряють потоки трафіку на предмет наявності пакетів, відповідних сигнатурам, які відповідають відомим їм загрозам. Але єдиний спосіб, яким вони можуть виявити, наприклад, морфіруючу шкідливу програму, – це продовжувати додавати все більше і більше сигнатур. Ще одна перевага автономної IPS пов'язано з продуктивністю мережі. Більшість мереж NGFW з вбудованою IPS і деякі традиційні автономні системи IPS зазнають труднощів з масштабуванням для досягнення продуктивності центру обробки даних. Наприклад, включення елементів управління додатками і можливостей механізму IPS зіставлення сигнатур може значно знизити продуктивність в більшості NGFW. Більш складна технологія IPS і дешифрування SSL, реалізовані в брандмауері, можуть привести до ще більшого зниження продуктивності [12].

Організації з високими вимогами до продуктивності можуть в кінцевому підсумку вирішити, що для досягнення вимог компанії потрібно розгортання автономного NGIPS разом з NGFW.

Варіант 2: перехід до можливостей IPS в рамках брандмауера. Більшість аналітиків згодні з тим, що ринок автономних рішень IPS або зупинився, або скорочується. Це пов'язано з тим, що в багатьох філіях і кампусах консолідуються свої пристрої безпеки і реалізуються NGFW, що містять відповідні NGIPS. Об'єднання брандмауера, віртуальної приватної мережі (VPN), антивіруса і IPS в одному пристрої привертає увагу, особливо для організацій, які вирішили скоротити витрати, спростити управління своїми пристроями і усвідомлюють брак співробітників служби безпеки. Це спонукає деяких аналітиків до висновку про смерть автономних IPS [12].

Невеликі філії і містечка середнього розміру, відокремлені від

корпоративного центру обробки даних, переходять на IPS в рамках NGFW. Якщо особи, які приймають рішення в області безпеки, задоволені рівнем функціональності і продуктивності IPS, який забезпечує NGFW, має сенс вказати рішення IPS-in-NGFW. При цьому важливо, щоб організація провела відповідну оцінку ризиків і тестування, щоб переконатися, що пропускна здатність і продуктивність з активним з'єднанням IPS відповідають очікуванням або перевершують їх.

У міру того, як директора з мережевої безпеки вивчають варіанти побудови та застосування IPS і оцінюють такі кроки, їх ключові міркування повинні включати:

рівень складності безпеки, необхідний їх мережі;

пропускна здатність, необхідна для брандмауера і IPS – незалежно від того, що один пристрій;

проблеми з витратами і персоналом.

IPS, як правило, розгортається «в лінії», де вони розташовуються на прямому шляху зв'язку між джерелом і пунктом призначення, де система може аналізувати в реальному часі весь потік мережевого трафіку по цьому шляху і вживати автоматизованих профілактичних дій. IPS можна розгорнути в будь-якій точці мережі, але їх найпоширеніші розгортання:

Enterprise Edge, периметр;

центр обробки даних підприємства.

IPS можна застосувати як автономну IPS або ж цю функцію можна ввімкнути в консолідовані функції IPS всередині брандмауера наступного покоління (NGFW). IPS використовує сигнатури, які можуть бути як вразливістю, так і експлуатуватись специфічно для ідентифікації шкідливого трафіку. Зазвичай це виявлення на основі сигнатури або виявлення на основі статистичної аномалії для виявлення шкідливої діяльності.

Виявлення на основі сигнатур використовує однозначно ідентифікувані сигнатури, які містяться в коді експлойту. Коли виявляються рухи, їх сигнатури потрапляють у базу даних, яка все більше розширюється. Виявлення сигнатур на

основі IPS включає або сигнатури, спрямовані на експлуатацію, які ідентифікують самі експлойти, або сигнатури, що стикаються з уразливістю, які визначають вразливість системи, на яку спрямовано атаку. Сигнатури, що стикаються з уразливістю, важливі для виявлення потенційних варіантів експлуатації, які раніше не спостерігались, але вони також збільшують ризик помилково позитивних результатів (доброякісні пакети, помилково позначені як загрози).

Статистичне виявлення на основі аномалії випадково відбирає мережевий трафік, а потім порівнює вибірки з базовими рівнями продуктивності. Коли зразки виявляються поза межами базової лінії, IPS запускає дію, щоб запобігти потенційній атаці.

Як тільки IPS ідентифікує зловмисний трафік, який може бути використаний мережею, вона розгортає так званий віртуальний патч для захисту. Віртуальний патч діє як засіб безпеки проти загроз, які використовують відомі та невідомі вразливості. Віртуальне виправлення працює шляхом реалізації рівнів політик та правил безпеки, які запобігають та перехоплюють експлойт від проходження мережевих шляхів до та від уразливості, забезпечуючи тим самим покриття проти цієї вразливості на рівні мережі, а не на рівні хоста.

Мережеві екрани FortiGate від Fortinet забезпечують комплексне рішення IPS, яке можна застосувати як окрему IPS, так і як консолідовану IPS в мережевому екрані. Перевірений лабораторіями NSS та іншими сторонніми службами оцінки, FortiGate IPS забезпечує високу ефективність безпеки з неперевершеною пропускною здатністю IPS і доступний у пристроях, віртуальних машинах та хмарі.

2.3. Принципи роботи рішення FortiGate IPS

Рішення NGFW FortiGate надають кращі в своєму класі можливості IPS для мережевої інфраструктури, заснованої на безпеці, забезпечуючи тонкий баланс та високу ефективність безпеки без порушення бізнес-процесів [9].

Треба підкреслити, що *рішення FortiGate IPS побудоване на унікальній архітектурі спеціалізованих процесорів безпеки і мережевих процесорів, які дозволяють йому забезпечувати безпрецедентну продуктивність в поєднанні з*

можливостями FortiGuard Labs [9].

Як в автономних системах IPS, так і в конвергентних міжмережевих екранах нового покоління інноваційна система FortiGate IPS забезпечує надійний захист світового класу. Завдяки виділеним блокам обробки даних для забезпечення безпеки і сучасної ефективної архітектурі продуктивність навіть в найбільших центрах обробки даних залишається стабільною. Автоматизовані процеси безпеки і експлуатації дають фахівцям з безпеки більше часу, щоб зосередитися на інших потребах, які потребують ручного втручання. Як частина Fortinet Security Fabric, FortiGate IPS використовує глобальну і локальну аналітику безпеки з іншими рішеннями Fortinet і довіреними сторонніми продуктами, забезпечуючи оцінку ризиків з використанням самої останньої інформації, а також поліпшення загального стану безпеки [9].

Перевагами FortiGuard IPS є [9]:

більш 13000 сигнатур вразливостей і експлойтів;

захист від вразливостей нульового дня;

більш швидкий час захисту з щоденним оновленням сигнатур IPS.

Автоматичні оновлення IPS FortiGuard забезпечують актуальний захист від мережевих вторгнень, виявляючи і блокуючи загрози до того, як вони досягнуть мережевих пристроїв. FortiGate IPS є новітнім засобом захисту від прихованих загроз мережевого рівня, має велику бібліотеку IPS з тисячами сигнатур, гнучкі політики, що забезпечують повний контроль над методами виявлення атак відповідно зі складними додатками безпеки, стійкість до методів ухилення (що доведено NSS Labs) і службу пошуку сигнатур IPS [9].

Більшість моделей FortiGate мають *спеціалізоване апаратне прискорення* (так зване блоки обробки даних), яке може вивантажувати інтенсивну обробку ресурсів з основних ресурсів обробки (Security Processing Units, SPUs)). Більшість компонентів FortiGate включають спеціалізовані процесори контенту (CP), які прискорюють широкий спектр важливих процесів безпеки, таких як сканування вірусів, виявлення атак, шифрування та дешифрування. Тільки вибрані моделі початкового рівня FortiGate не включають процесор CP [8].

Багато моделей FortiGate також містять процесори безпеки (SP), які прискорюють обробку для певних функцій безпеки, таких як IPS та мережеві процесори (NP), які розвантажують обробку великого обсягу мережевого трафіку.

Розглянемо апаратне забезпечення блоку обробки даних (Security Processing Unit, SPU), яке Fortinet вбудовує в пристрої FortiGate для прискорення трафіку через блоки FortiGate. Існують три типи SPU:

процесори контенту (Content processors, CPs), які прискорюють широкий спектр функцій безпеки

процесори безпеки (Security processors, SPs), які прискорюють певні функції безпеки

мережеві процесори (Network processors, NP і NPlites), які розвантажують мережевий трафік до спеціалізованого обладнання, оптимізованого для забезпечення високого рівня пропускної здатності мережі.

Розглянемо архітектуру на прикладі рішень FortiGate 200E and 201E (рис. 2.3).

FortiGate 200E та 201E включають два процесори SOC3 NP6XLite. Процесори SOC3 та процесори CP9Lite не використовуються. Натомість архітектура FortiGate 200E та 201E включає окремі ресурси процесора та стандартний процесор CP9 [8].

Оскільки ця модель не включає комутаційну структуру, то не можна створити групи агрегації посилань (Link Aggregation Groups, LAG) або надлишкові інтерфейси між інтерфейсами, підключеними до різних NP6Lites. Окрім того, трафік буде вивантажений лише в тому випадку, якщо він входить і виходить із FortiGate через інтерфейси, підключені до того ж NP6Lite.

NP6Lites підключені до мережевих інтерфейсів наступним чином:

NP6Lite_0 підключений до шести інтерфейсів 1GE RJ-45 (port9-port14)) та чотирьох інтерфейсів 1GE SFP (port15-18);

NP6Lite_1 підключений до десяти інтерфейсів 1GE RJ45 (wan1, wan2, port1-port8).

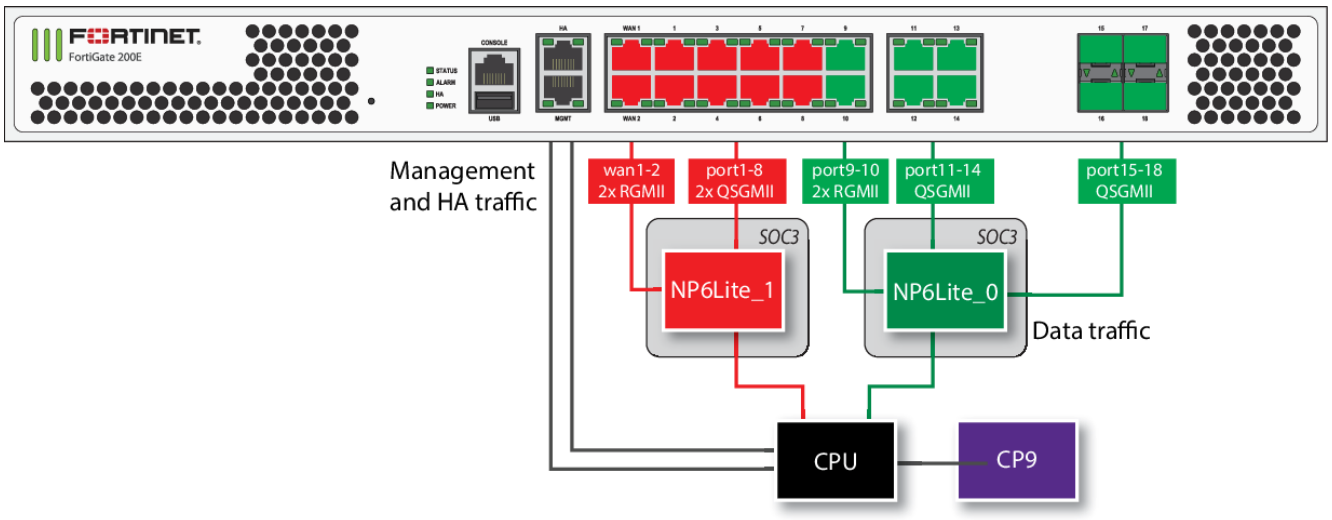

Рис. 2.3. Архітектура рішення FortiGate 200E [8]

Процесори контенту CP9, CP9XLite (застосовуються в SOC4) та CP9Lite (застосовуються в SOC3) підтримують переважно однакові функції, за деякими винятками, зазначеними нижче. Основна різниця між процесорами – це їх потужність і пропускна здатність. Наприклад, CP9 має шістнадцять механізмів IPsec VPN, тоді як CP9XLite – п'ять, а CP9Lite – один. Як результат, CP9 може прискорити набагато більше сесій IPsec VPN, ніж простіші версії [8].

Процесор контенту CP9 надає такі послуги [8]:

інспекція на основі потоку (IPS та контроль додатків) прискорення, що відповідає шаблону, з перепускною здатністю понад 10 Гбіт/с;

попереднє сканування IPS/розвантаження перед матчем;

розвантаження сигнатурної кореляції IPS;

розвантаження повного узгодження (лише CP9);

глибока перевірка пакетів на основі DFA;

високопродуктивний механізм масових даних VPN:

процесор протоколів IPsec та SSL/TLS;

DES/3DES/AES128/192/256 відповідно до FIPS46-3/FIPS81/FIPS197;

MD5/SHA-1/SHA256/384/512-96/128/192/256 з RFC1321 та FIPS180;

генерація MS/KM (хеш) (лише CP9);

HMAC відповідно до RFC2104/2403/2404 та FIPS198;

мод ESN;

підтримка GCM для NSA «Suite B» (RFC6379/RFC6460), включаючи

GCM-128/256; GMAC-128/256;

процесор обміну ключами, який підтримує високопродуктивні обчислення IKE та RSA:

механізм посилення відкритого ключа з підтримкою апаратної CRT;

первинна перевірка для генерації ключа RSA;

прискорювач рукостискання з автоматичною генерацією ключових матеріалів;

справжній генератор випадкових чисел (TRNG) з джерелом ентропії PLL (лише CP9 та CP9XLite);

кільце джерела ентропії OSC;

підтримка криптографії еліптичної кривої ECC (P-256) для NSA «Suite B» (лише CP9);

механізм допоміжного відкритого ключа (PKCE) для безпосередньої підтримки роботи до 4096 біт (4k для DH та 8k для RSA з CRT);

підтримка fingerprint DLP:

налаштовувані фрагменти контенту з двома порогами-двома дільниками (Two-Thresholds-Two-Divisors, TTTD).

Мережеві процесори FortiASIC працюють на рівні інтерфейсу, щоб прискорити трафік, вивантажуючи трафік з основного процесора. Сучасні моделі містять мережеві процесори NP6, NP6XLite та NP6Lite.

NP6Lite схожий на NP6, але з меншою пропускною здатністю та деякими функціональними обмеженнями (наприклад, NP6Lite не розвантажує трафік CAPWAP). NP6Lite є компонентом Fortinet SOC3. NP6Lite має максимальну пропускну здатність 10 Гбіт/с із використанням 2х інтерфейсів QSGMII та 2х RGMII.

NP6Lite працює так само, як NP6. Будучи легшою версією, NP6Lite має меншу ємність, ніж NP6. Максимальна пропускна здатність NP6Lite становить 10 Гбіт/с із використанням 2-х інтерфейсів QSGMII та 2-х зменшених гігабітних незалежних від носіїв інтерфейсів (RGMII).

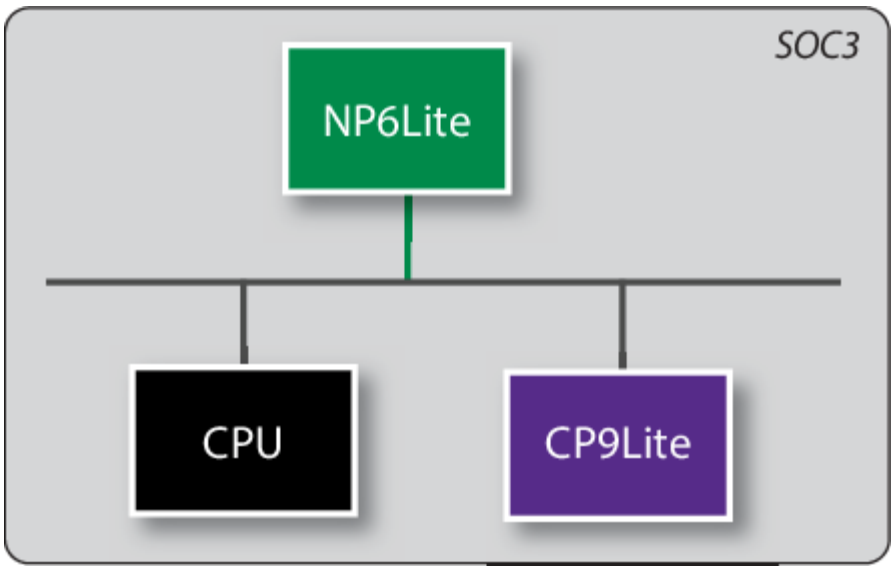

Рис. 2.4. Архітектура SOC3 [8]

Крім того, NP6Lite не розвантажує наступні типи сеансів CAPWAP, Syn proxy та помічника сеансу DNS.

NP6Lite є компонентом Fortinet SOC3 (рис. 2.4). SOC3 включає процесор, мережевий процесор NP6Lite та процесор контенту CP9Lite, який підтримує більшість функцій CP9, але з меншою ємністю.

3 ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ПОПЕРЕДЖЕННЯ ВТОРГНЕНЬ В КОРПОРАТИВНУ МЕРЕЖУ

3.1. Обгрунтування необхідності втілення та застосування системи попередження вторгнень в корпоративну мережу

Необхідно зазначити, що хоча щороку пишеться більше 100 мільярдів рядків нового програмного коду, кількість вразливостей в системі безпеки залишається незмінним протягом останніх двох десятиліть – в середньому 26,7 критичних вразливостей на додаток. Згідно зі звітом Verizon про розслідування витоків даних за 2020 рік, майже половина (43%) всіх успішних витоків даних може бути пов'язана з уразливостями додатків – частка, яка збільшилася більш ніж удвічі за рік. Вразливості можна використовувати за допомогою різних форм атак, таких як злом, соціальна інженерія, шкідливе ПЗ і боти [10].

Ефективна система запобігання вторгнень (IPS) може допомогти захистити як відомі, так і заздалегідь виявлені (нульового дня) вразливості від експлуатації. Міжмережеві екрани наступного покоління (NGFW) FortiGate включають можливості IPS і навіть можуть бути розгорнуті як спеціалізоване рішення IPS [10].

Рішення FortiGate IPS, оснащений спеціалізованими процесорами безпеки, які підвищують продуктивність, і провідним аналізатором загроз від FortiGuard Labs, який забезпечує швидкий і ефективний захист від вразливостей [10].

«Вразливість» зазвичай асоціюється з невстановленим програмним забезпеченням і неправильною конфігурацією. Це може відноситися до помилки або вразливості в коді програми, інтерфейсу прикладного програмування (API), вбудованого ПЗ або операційної системи, які потім можуть бути використані для отримання несанкціонованого доступу до базової системи. Успішне використання вразливості дозволяє зловмисникам запустити в системі неперевірений і шкідливий код і отримати доступ до системної пам'яті або отримати доступ адміністратора на рівні системи для інсталяції шкідливого ПЗ [10].

Зловмисники використовують різні методи, включаючи впровадження (наприклад, SQL, мова виразів NoSQL), переповнення буфера, міжсайтовий скриптинг (XSS), обфускація Java та інші методи для приховування шкідливого коду [10].

«Експлойт» відноситься до інструменту, що використовується для зловмисної атаки на вразливість. Сам експлойт зазвичай являє собою частину програмного забезпечення, фрагмент даних або послідовність команд, які використовують додаток або систему, щоб викликати передбачене або непередбачене поводження. Комплекти експлойтів (або пакети експлойтів) – це автоматизовані програми, які використовуються зловмисниками для експлуатації відомих вразливостей в системах або додатках [10].

Їх можна використовувати для таємного запуску атак, поки жертви переглядають веб-сторінки, з метою завантаження і виконання будь-якого шкідливого ПЗ. Складні набори експлойтів здатні атакувати безліч різних вразливостей в кількох додатках [10].

Одна вразливість може використовуватися по-різному. Вона може мати відношення «один до багатьох» з експлойта, коли кілька експлойтів можуть по-різному впливати на одну вразливість або вона може мати відношення «багато до одного», коли один експлойт може одночасно використовувати кілька різних вразливостей [10].

Оскільки вразливості продовжують залишатися основною причиною порушень, більшість підприємств постійно відстежують і виправляють вразливості для запобігання експлуатації. При виявленні нової вразливості розробник програмного забезпечення повинен швидко розробити і випустити виправлення для усунення проблеми. Після цього IT-відділ організації повинен діяти швидко, щоб виправлення було розгорнуто на всіх примірниках додатку в інфраструктурі. Це вікно може пропонувати зловмисникам необхідний час для настройки і запуску атаки на виявлену вразливість [10].

Гірше того, існують також схильні (або «нульові») вразливості – невиявлені помилки або недоробки, для яких немає виправлень. Використання вразливостей

нульового дня може зайняти дні або місяці, перш ніж вони будуть виявлені, що може дати зловмисникові досить часу, щоб завдати серйозної шкоди організації. Отже, навіть найсуворіші стратегії управління виправленнями не можуть повністю усунути ризики відомих вразливостей або вразливостей нульового дня.

FortiGate IPS захищає вразливості від експлуатації. *Для захисту як відомих вразливостей, так і вразливостей нульового дня від експлуатації організаціям необхідна система запобігання вторгнень (IPS) наступного покоління, яка працює як інтегрована частина їх більш широкої архітектури безпеки* [10].

Fortinet надає перевірені в галузі можливості IPS через платформу FortiGate – використовуючи існуючий NGFW FortiGate зі службою FortiGate IPS або розгортаючи виділений FortiGate як автономного рішення IPS. FortiGate IPS поєднує в собі продуктивність процесорів безпеки FortiGate з декількома механізмами перевірки, потоками аналітичних даних про загрози і розширеними можливостями загроз для захисту вразливостей від атак. Це включає в себе віртуальне виправлення, яке захищає вразливості на мережевому рівні за допомогою сигнатур IPS [10].

З більш ніж 13000 сигнатур IPS та оновленнями в реальному часі від FortiGuard Labs FortiGate IPS допомагає організаціям швидше реагувати на новітні загрози, пропонуючи при цьому повний захист від усіх типів вразливостей. Перш за все, FortiGate IPS створений для швидкості. Захист відбувається на швидкості лінії – так само, як і на автономних пристроях IPS. Механізм IPS Fortinet автоматично перевіряє пакети і застосовує фільтри до контенту, що проходить через операційну систему FortiOS. Після того, як механізм IPS ідентифікує шаблон, він потім перекладає повний процес зіставлення сигнатур на процесор контенту FortiGate, щоб підтримувати оптимальний захист мережі [10].

Швидка доставка сигнатур на основі FortiGuard Labs – ще одне ключова перевага, яку пропонує Fortinet. FortiGate IPS отримує вигоду з досліджень загроз на основі штучного інтелекту (ШІ), що проводяться FortiGuard Labs щодо як відомих, так і нових вразливостей. На основі останніх даних телеметрії FortiGuard Labs створює попереджувальні сигнатури для виявлення будь-яких експлойтів

вразливості до того, як постачальник випустить виправлення. Це дозволяє FortiGuard Labs інформувати FortiGate IPS (та всі інші інтегровані компоненти Fortinet Security Fabric) щодо останніх даних про загрози [10].

Сигнатури FortiGate IPS оновлюються щодня після ретельного тестування і перевірки, щоб звести до мінімуму помилкові спрацьовування. У більшості випадків сигнатура будь-якої нової критичної вразливості доставляється протягом 48 годин після виявлення. Для багатьох конкуруючих рішень щотижневі оновлення є нормою, що розширює вікно потенційної експлуатації [10].

FortiGate IPS також використовує машинне навчання (ML) для виконання автоматичного аналізу сигнатур для розширеного захисту від атак ботнетів. З приходом буквально мільйонів сигнатур ботнетів ML пропонує інтелектуальний інструмент для виявлення вразливостей, які можуть бути схильні до атак за допомогою спамерських пошукових роботів [10].

Необхідно підкреслити, що NSS Labs також зазначила, що FortiGate IPS пропонує найкращу сукупну вартість володіння (TCO) – важливе міркування при спробі захистити підприємство від новітніх загроз з обмеженими ресурсами. Як частина Fortinet Security Fabric, FortiGate IPS допомагає захистити всю інфраструктуру організації від початку до кінця. FortiGate IPS отримує вигоду з обміну даними з іншими продуктами Fortinet, а також з продуктами партнерів. Наприклад, FortiGate IPS працює з такими рішеннями, як FortiClient (захист кінцевих точок) і FortiSandbox (пісочниця), щоб виявляти невідомі вразливості в реальних умовах (наприклад, нові варіанти шкідливих програм), а потім перетворювати їх в відомі загрози за допомогою дослідження FortiGuard Labs [10].

FortiGate IPS також використовує розширену аналітику і робочі процеси політик через FortiAnalyzer. Ці ключові інтеграції роблять розслідування і реагування на інциденти більш продуктивними, оскільки вони можуть відбуватися в контексті всієї архітектури Security Fabric, а не у вигляді ізольованих даних від автономного пристрою IPS або датчика брандмауера [10].

Крім того, FortiGate IPS – це багате джерело криміналістичних даних, які в рівній мірі доступні для інших рішень Security Fabric, що, в свою чергу, допомагає

зміцнити загальний стан безпеки організації. У зв'язку з цим FortiGate IPS дає підприємствам можливість виявляти, ізолювати і усувати критичні уразливості, де б вони не знаходилися [10].

3.2. Рекомендації щодо застосування технолгії попередження вторгнень в корпоративну мережу

Системи запобігання вторгнень (IPS) лежать в основі безпеки корпоративних центрів обробки даних і інших місць, де важлива безпека. Але для одних компаній різні пристрої IPS працюють краще, ніж для інших [13].

Вибір правильного рішення IPS для конкретного об'єкта вимагає ретельного розгляду різних питань, від масштабованості і продуктивності до включення аналітики загроз і здатності захищати дані і додатки як в загальнодоступних, так і в приватних хмарах [13].

Компанії можуть впроваджувати IPS або через автономні пристрої IPS, або через міжмережеві екрани наступного покоління (NGFW), які включають функції IPS. Автономні пристрої, як правило, забезпечують більш надійні можливості перевірки і більш високу продуктивність. З іншого боку, використання IPS, інтегрованого в NGFW, спрощує адміністративні задачі і може знизити витрати. Сума економії залежить від того, скільки інших функцій NGFW включено на тому ж пристрої, і від пропускної спроможності, необхідної компанії. В цілому, вимоги до продуктивності і безпеки диктують відповідний форм-фактор IPS [13].

Ринки як автономних, так і інтегрованих в NGFW IPS швидко змінюються. Деякі постачальники розширюють свою присутність в цій сфері, в той час як інші продають або припиняють випуск своїх технологій IPS. Вирішальне значення має пошук рішень IPS, які забезпечують більшу відповідність рядків і складні набори сигнатур для блокування відомих вразливостей [13].

За останні кілька років деякі постачальники розширили свою присутність в цій сфері, в той час як інші продали або припинили випуск своїх технологій IPS.

У 2017 році IBM оголосила про закінчення продажу своєї лінійки продуктів для мережевої безпеки (XGS). Cisco також припинила випуск Cisco IPS, який

раніше продавався разом з міжмережевими екранами ASA. McAfee анонсувала про закінчення продажу для своїх пристроїв серії M і I. Trend Micro припиняє випуск своїх платформ серії S і NX [13].

Навіть серед постачальників, які залишаються прихильними ринку, технологія IPS змінюється так швидко, що практично потрібно періодичне оновлення обладнання.

Розглянемо характеристики успішної IPS. Перше, на що слід звернути увагу при оцінці перспективних IPS – це їх базовий набір функцій. Зіставлення сигнатур є фундаментальним для кожної IPS, тому директорам з безпеки необхідно розуміти механізм зіставлення сигнатур у кожній зі своїх опцій IPS.

Найголовніша форма сигнатури – це зіставлення рядків, коли сигнатура просто шукає точний збіг з відомими даними. *Такий підхід вимагає великих наборів сигнатур, оскільки постачальники повинні створювати нову сигнатуру не тільки для кожної нової загрози, а й для кожного різновиду цієї загрози.* Ці сигнатури будуть відповідати тільки одному корисному навантаженню [13].

Складні набори сигнатур включають списки відомих вразливостей, завдяки чому одна сигнатура може блокувати безліч різних варіантів атаки, націлених на ту ж саму вразливість. Такий підхід до сигнатур більш ефективний, ніж зіставлення рядків, і призводить до меншої кількості загальних сигнатур. Вивчення кількості сигнатур IPS і перехресних посилань на нього з показниками виявлення авторитетних сторонніх тестів (наприклад, NSS Labs) має визначити, що ці постачальники мають хороші показники і мають більш низьку кількість сигнатур.

Складні IPS доповнюють блоками контекстної інформації, такої як поведінка користувачів та евристика, виявлення аномалій мережевих і прикладних протоколів та інших відхилень від історичних норм. Ці функції розширюють можливості системи виявлення та запобігання вторгнень, зменшуючи кількість попереджень і помилкових спрацьовувань.

Серед рішень IPS, ефективних в цих областях, директор з безпеки повинен вибрати ті, які відповідають наступним вимогам [13]:

1. Масштабованість і продуктивність. Продуктивність є ключовим фактором,

що спонукає багато компаній вибирати автономну IPS, а не функціональність, інтегровану в NGFW. Додаткове навантаження на брандмауер, який тепер повинен перевіряти пакети і корисне навантаження на наявність IPS, сповільнить мережевий трафік.

Одне тільки зіставлення сигнатури може знизити швидкість деяких NGFW на цілих 30%. IPS необхідно масштабувати для збільшення обсягів трафіку як всередині центру обробки даних, так і на периметрі мережі. Є кілька способів, якими постачальники IPS можуть вбудувати масштабованість в свої пристрої.

Один з них полягає в включенні блоку обробки даних безпеки. Архітектура традиційних пристроїв безпеки на базі ЦП може стати вузьким місцем для брандмауера або IPS. Одному високопродуктивної процесору може бути важко задовольнити потреби мережі в високої пропускної здатності, а також вимоги безпеки для глибокого аналізу.

Особи, які приймають рішення в області безпеки, повинні ретельно продумати архітектуру, яка відокремлює обробку мережі від обробки безпеки, щоб ресурси можна було ефективно використовувати в міру необхідності, і один процес не був заручником іншого, що знижує пропускну здатність для обох процесів.

Можливість перевірки зашифрованого трафіку має вирішальне значення для будь-якої IPS. Однак це може бути надзвичайно ресурсномістким і багато постачальників не можуть домогтися цього на високій швидкості. В результаті різко знижується загальна пропускна здатність або, що ще гірше, IPS просто передає зашифрований трафік, не перевіряючи його.

Передача цього завдання з основного процесора на спеціалізований процесор контенту вирішує цю проблему. Хоча додавання процесора контенту до IPS не збільшує загальну пропускну здатність пристрою, воно знижує зниження продуктивності, яке може виникнути в результаті активації певних функцій безпеки, таких як дешифрування.

2. Можливості розширеного запобігання загрозам, засновані на аналітиці загроз. Розширене запобігання загрозам (ATP) призначене для виявлення шкідливих програм і програм-вимагачів, які спеціально націлені на проломи в

безпеці мережі. Це критично важлива функція.

Всього за три місяці 2017 року FortiGuard Labs повідомила про 14 904 нових шкідливих програмах – в середньому 160 на день.

Перспективні рішення IPS мають включати запобігання ATP. Також слід очікувати, що ці можливості ATP будуть інтегровані зі службою розвідки загроз. Деякі постачальники IPS мають свої власні можливості аналізу загроз, які доповнюють вбудовану функціональність пристроїв постійними оновленнями про нульового дня і інші загрози.

3. Видалення стін між NOC і SOC. Традиційно операційний центр безпеки (SOC) компанії функціонує окремо від центру управління мережею (NOC). У них різний персонал і різні процеси управління. Але такі розрізнені операції майже напевно приведуть до дублювання зусиль, можливо, навіть до персоналу, що працює з різними цілями.

Гірше того, бар'єри між NOC і SOC можуть підірвати загальний стан безпеки компанії. NOC містить великий обсяг інформації про корпоративні мережі, в тому числі про те, де запущено конкретний додаток і оновлено чи виправлено його. При виявленні атаки NOC може відповісти на питання про те, які кінцеві точки вразливі і наскільки тривожною повинна бути група безпеки. Ця інформація може мати життєво важливе значення для швидкої і ефективної відповіді на будь-який тип атаки.

NOC не вистачає інформації, необхідної для виявлення та викорінення цих атак. У SOC зберігаються докладні дані про виникаючі загрози, які допоможуть організації визначити потенційні атаки, перш ніж вони зможуть вплинути на корпоративні системи. Але SOC без бази знань NOC не має доступу до мережі, щоб персонал міг ефективно оцінити вразливість організації і відреагувати.

Недавнє опитування показало, що серед компаній, у яких є SOC, 22% не мають NOC, 12% повідомили, що їх команди NOC і SOC дуже мало спілкуються безпосередньо, а 21% заявили, що їх команди NOC і SOC працюють разом тільки під час виникнення небезпеки.

Найбільш ефективна система безпеки об'єднує дані з корпоративних NOC і

SOC. Компанії, яка набуває можливості IPS, слід шукати рішення, які усувають розрізненість NOC і SOC, об'єднуючи інформацію про загрози безпеці з даними про уразливість мережі.

4. Інтеграція в комплексну екосистему безпеки. Традиційно операційний центр безпеки (SOC) компанії функціонує окремо від мережевого операційного центру (NOC). У них різний персонал і різні процеси управління. Але такі розрізнені операції майже напевно приведуть до дублювання зусиль, можливо, навіть до персоналу, що працює з різними цілями. Ще одна причина тісної інтеграції рішень корпоративної безпеки – це оптимізація ефективності і мінімізація витрат.

Використання розрізнених систем часто означає, що співробітники повинні виконувати одні й ті ж завдання по-різному в різних системах. У той же час на виконання завдань йде більше часу, оскільки перехід від інтерфейсу одного рішення до іншого. Звичайно, в розрізнених сценаріях для прискорення підготовки нових співробітників потрібно більше часу, і компанії, можливо, навіть буде потрібно зберегти більшу команду безпеки для укомплектування всіх різних систем.

Навпаки, тісно інтегровані рішення, що пропонують аналогічні інтерфейси і робочі процеси, дозволяють співробітникам, що використовують одну систему, легко брати на себе управління іншою. Щоб оптимізувати як ефективність, так і результативність процесів безпеки своєї компанії, директорам з безпеки слід шукати рішення IPS, які інтегруються з іншими продуктами безпеки компанії, щоб забезпечити тісну функціональність і прозору видимість.

5. Використання хмар. І нарешті, необхідно розглянути можливість захисту додатків і даних в хмарі. Практично кожна компанія використовує хмарні додатки в тій чи іншій формі, а в більшості – досить багато. Fortinet виявила, що типова компанія використовує 62 різних додатки в хмарі.

Інше недавнє дослідження показало, що 85% організацій з більш ніж 1000 співробітників використовують більше одноєї хмари – кілька загальнодоступних хмар, кілька приватних хмар або гібридне середовище.

Таким чином, логічно припустити, що рішення IPS має не тільки захищати локальне програмне забезпечення і дані, а також мати можливість працювати як в загальнодоступних, так і в приватних хмарах. В рамках процесу комплексної перевірки директор з безпеки повинен оцінити, де знаходяться дані і додатки компанії, а також здатність перспективних рішень IPS захистити їх, незалежно від місця розташування [13].

Прийняття рішення. Незважаючи на терміновість мінімізації ризику, особливо з урахуванням нестабільності ринку IPS, директорам з безпеки не слід поступатися належною обачністю при виборі системи IPS. Вони повинні гарантувати, що їх перспективні рішення IPS будуть масштабуватися з урахуванням як поточної здатності, так і прогнозованого майбутнього зростання.

Вони повинні оцінити, чи будуть ці системи ефективно інтегруватися в їх поточну екосистему безпеки або створять (або збережуть) проблему розрізненості інформації. Також вони повинні враховувати питання ціни і продуктивності.

Що потрібно робити організаціям? Деякі організації прокидаються, тому що цей новий світ кіберзагроз реальний і нікуди не дінеться. Вони прийняли нову мантру, яка визнає, що кіберпідготовка повинна фокусуватися не на «якщо», а на «коли» вони стають метою. Це означає, що їх ресурси повинні бути зосереджені не тільки на проактивному захисту, але і на ефективному реагуванні на інциденти. Це тому, що вони розуміють, що злом неминучий, а захист мережі залежить від знання, що робити далі, щоб зупинити цю атаку [7].

Ефективна і інтегрована система штучного інтелекту наступного покоління надає найкращі можливості для захисту мереж і реагування на атаки до досягнення своїх цілей. Він повинен функціонувати аналогічно адаптивної імунної системи, яка захищає наші тіла від хвороб, бореться з інфекціями, коли наші тіла знаходяться під загрозою, і модифікує цю імунну систему, щоб боротися з тими ж вірусами в майбутньому [7].

Згідно з [2] розглянемо найкращі рекомендацій організаціям та підприємствам щодо забезпечення кібербезпеки.

1. Розробити та впровадити методологію кібербезпеки (threat-based

cybersecurity, TBC), засновану на загрозах: проактивний підхід до визначення цінних даних, оцінки зберігання та передачі даних на наявність уразливих місць та зменшення найбільш вірогідних ризиків та векторів атак. Це максимізує ефективність ресурсів кібербезпеки, зосереджуючись на унікальному профілі загроз організації.

Досягнення цього відбувається як частина постійного процесу, який реагує на нові кіберзагрози. MITRE рекомендує наступні кроки для впровадження методології TBC:

отримати інформацію та аналіз кіберзагроз;

забезпечити захист від визначених загроз;

здійснення цілеспрямованого обміну та співпрацю інформації про кіберрозвідку та атаки.

2. Перехід до керованих послуг з кібербезпеки: урядові установи, організації та підприємства дедалі частіше усвідомлюють цінність передачі послуг з кібербезпеки на аутсорсінг та використовують комерційні готові послуги (commercial off-the-shelf, COTS), що надаються досвідченими системними інтеграторами та постачальниками керованих служб безпеки (managed security service provider, MSSP). SI та MSSP можуть надати експертного досвіду та перевірені ефективні технології кібербезпеки для збільшення використання автоматизації даних, автоматизації робочих процесів, аналізу великих даних та візуалізації даних для підвищення продуктивності та економічної ефективності.

Переходячи від підрядника з кібербезпеки, бізнес-модель збільшення персоналу до моделі послуг з керованою кібербезпекою вимагає часу для планування, вибору правильних показників ефективності та показників та забезпечення плавного переходу.

Типові послуги, керовані кібербезпекою, включають: послуги операційних центрів безпеки (security operation center, SOC), послуги інформації про безпеку та управління подіями (security information and event management, SIEM), управління реагуванням на інциденти (incident response management, IRM), управління вразливістю та розвідка кіберзагроз (cyber threat intelligence, CTI) тощо.

3. Необхідно навчати фахівців з безпеки та проводити тренінги: скористайтеся можливостями хмарних сервісів з емуляційними мережами інформаційних систем та модельованими кібератаками, щоб забезпечити стійку кіберпросвіту та навчання для спеціалістів у поєднанні з настільними вправами для керівництва організацій.

4. Створіть середовище даних «нульової довіри» («zero trust»): перехід до середовища захисту даних нульової довіри з політиками, планами та архітектурою нульового довіри (ZTA), що включає мікросегментацію даних, мікроперіметри, шлюзи сегментації даних, ICAM до меж тощо.

5. Необхідно впровадити систему виявлення вторгнень (IDS), керовану штучним інтелектом (artificial intelligence, AI): впровадити нове програмне забезпечення з використанням можливостей AI та ML для більш точного моніторингу трафіку електронної пошти, мережі та кінцевих точок для виявлення підозрілої діяльності та чітких загроз у реальному часі.

6. Необхідно розробити та протестувати внутрішній та зовнішній план комунікацій щодо порушення кіберданих: узгодити існуючі рамки управління ризиками підприємств (тобто за стандартами NIST SP 800-37 та NIST SP 800-53).

7. Необхідно впровадити та протестувати план реагування на кібернетичні інциденти: включити участь керівництва організації та ключового персоналу з усіх технологій, ділового адміністрування та інших функцій.

8. Необхідно впровадити ідентифікацію, облікові дані та управління доступом (identity, credential and access management, ICAM) на всьому підприємстві: розробити технічну політику та процедури, щоб забезпечити доступ лише уповноважених працівників до конфіденційної інформації (sensitive information, SI), контрольованої некласифікованої інформації (CUI та персональної інформації, що ідентифікує особу (personal identifiable information, PII). Потім, впровадити наскрізне програмне забезпечення ICAM із вдосконаленим програмним шифруванням, багатофакторною автентифікацією (multifactor authentication, MFA) із використанням парольних фраз та біометрії, а також меж на основі облікових даних або меж на основі ролей.

9. Створіть програму протидії інсайдерським загрозам: включити політики, освіту, навчання, моніторинг, виявлення та реалізацію архітектури нульового довіри, яка створює мікро-периметри та сегментацію даних, щоб обмежити внутрішній вертикальний та бічний рух в межах інформаційної системи, доступ лише затвердженим особам.

10. Складіть і протестуйте план безперервності бізнесу (business continuity plan, BCP): для того, щоб забезпечити справжню стійкість до інформації, життєво важливо мати ефективну можливість резервного копіювання інформації.

Таким чином, для урядових установ, організацій та підприємств важливо впровадити перевірені найкращі практики з кібербезпеки, щоб стати невід'ємною частиною планування цифрових трансформацій та зусиль із впровадження, щоб забезпечити конфіденційність даних та стійкість даних.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми попередження вторгнень в корпоративну мережу. Розвиток корпоративних мережевих інфраструктур призвів до розширення поверхні атаки для відомих, невідомих та загроз нульового дня. Оскільки першопричини більшості порушень пов'язані з використанням відомих вразливостей, багато організацій, щоб не відставати, застосовують системи запобігання вторгнень (IPS).

Проведено аналіз існуючих методів та засобів виявлення та попередження вторгнень в корпоративну мережу та встановлено, що найбільш перспективним є застосування технології IPS. Правильна IPS пропонує найбільш ефективний спосіб блокувати загрози, які використовують відомі вразливості. В сучасній IPS застосовуються різні методи виявлення загроз, зокрема, поведінковий – відомий як виявлення аномалій та інтелектуальний – відомий як виявлення по сигнатурам або виявлення несанкціонованого використання.

Досліджено методи та засоби виявлення та попередження вторгнень в інформаційну систему підприємства на прикладі рішення FortiGate IPS. Встановлено, що рішення NGFW FortiGate надають кращі в своєму класі можливості IPS для мережевої інфраструктури, заснованої на безпеці, забезпечуючи тонкий баланс та високу ефективність безпеки без порушення бізнес-процесів. Треба підкреслити, що рішення FortiGate IPS побудоване на унікальній архітектурі спеціалізованих процесорів безпеки і мережевих процесорів, які дозволяють йому забезпечувати безпрецедентну продуктивність в поєднанні з можливостями FortiGuard Labs.

Розглянуто порядок втілення та застосування системи виявлення та попередження вторгнень в інформаційну систему підприємства на прикладі рішення FortiGate IPS.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо вибору та застосування системи попередження вторгнень в корпоративну

мережу.

Від правильного визначення умов функціонування інформаційної системи підприємства, вибору та обґрунтування складу методів та засобів виявлення та попередження вторгнень та ефективного їх застосування залежить ефективність забезпечення кібербезпеки корпоративних мереж.

Таким чином, запропоновані в роботі рекомендації мають сприяти підвищенню захищеності функціонування корпоративної мережі шляхом втілення та застосування методів та засобів виявлення та попередження вторгнень.

ПЕРЕЛІК ПОСИЛАНЬ

1. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. /Carson Zimmerman –The MITRE Corporation, 2014. – 346 p.

2. 2021 cybersecurity trends and recommendations. Special focus: U.S. public sector [Електронний ресурс] – Режим доступу: https://perspecta.com/sites/default/files/2021-01/Cybersecurity%202021%20trends%20and%20rec%20wp_online.pdf.

3. Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft). Recommendations of the National Institute of Standards and Technology. Karen Scarfone. Peter Mell. National Institute of Standards and Technology Special Publication 800-94 Revision 1 (Draft), 111 pages (Jul. 2012) https://csrc.nist.gov/csrc/media/publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf.

4. How much would a data breach cost your business? [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/data-breach.

5. U.S. government and cyber crime – Statistics & Facts. Published by J. Clement, Jul 22, 2020 [Електронний ресурс] – Режим доступу: https://www.statista.com/topics/3387/us-government-and-cyber-crime/.

6. X-Force Threat Intelligence Index 2021. IBM Security [Електронний ресурс] – Режим доступу: https://www.ibm.com/security/data-breach/threat-intelligence.

7. Cyber Threat Predictions for 2021. An Annual Perspective by FortiGuard Labs. White Paper [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-cyber-threat-predictions-for-2021.pdf.

8. Hardware Acceleration Guide FortiOS 7.0.0 [Електронний ресурс] – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/54ac6091-922e-11eb-b70b-00505692583a/fortios-hardware-acceleration-700.pdf.

9. Protect Against Known and Unknown Threats with FortiGate IPS and FortiGuard IPS Service. Solution Brief [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-protect-against-known-and-unknown-threats-with-fortigate-ips.pdf.

10. Mitigating Vulnerabilities: A FortiGate IPS Overview. Solution Brief [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-mitigating-vulnerabilities-fortigate-ips-overview.pdf.

11. Proactive Threat Protection with FortiGate IPS. Solution Brief [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-proactive-threat-protection-with-fortigate-ips.pdf.

12. IPS: Out With The Old, In With The New. Two Options for Evolving your IPS Solution. White Paper [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-ips-out-with-the-old-in-with-the-new.pdf.

13. A Definitive Guide To The IPS Technology Landscape. Essential Solution to Selection Criteria. White Paper [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/white-papers/wp-a-definitive-guide-to-the-ips-technology-landscape.pdf.

14. Powerful and Innovative Intrusion Prevention Systems. FortiGate IPS. Solution Brief [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-FortiGateIPS.pdf.

15. Павловський Олексій Юрійович. Технологія попередження вторгнень в корпоративну мережу на базі FortiGate IPS. ВСЕУКРАЇНСЬКА НАУКОВА КОНФЕРЕНЦІЯ «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ». Державний Університет Телекомунікацій. 27 жовтня 2021. Тези доповідей. С. 43 – 46. http://www.dut.edu.ua/uploads/p_2099_79407917.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)