ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ СИСТЕМИ РОЗПОДІЛЬНОГО МОНІТОРІНГУ СТАНУ КОРПОРАТИВНИХ МЕРЕЖ ZABBIX »

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Додонов К. М.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

СЗІ – система захисту інформації

AD – Active Directory

AML – Advanced Machine Language

AEP – Advanced Endpoint Protection

APT – Advanced Persistent Threats

CPU – Central Processing Unit

DDoS – Distributed Denial of Service

IRP – Incident Response Platforms

IPS – Intrusion Prevention System

IDS – Intrusion Detection System

IoT – Internet of Things

IdM – Identity Management

IAM – Identity and Access Management

IPMI – Intelligent Platform Management Interface

DLP – Data Leak Prevention

EDR – Endpoint Detection and Response

HTTP – HyperText Transfer Protocol

UDP – User Datagram Protocol

TCP – Transmission Control Protocol

SIEM – Security information and event management

SMS – Short Message Service

ВСТУП

Актуальність дослідження. Сьогодення, інформаційні системи стають невід'ємною частиною системи управління та моніторингу, в тому числі, при забезпеченні захисту кібербезпеки.

Останнім часом, частота несанкціонованих впливів на інформаційні системи постійно збільшується, що неминуче призводить до величезних фінансових і матеріальних втрат. Підтвердженням цьому є дані щорічних досліджень Інституту комп'ютерної безпеки США, які показують велику кількість успішних вторгнень в інформаційних системи за останні роки. Безпека інформаційних систем є частиною більш широкої проблеми, такої, як захист корпоративних мереж, комп'ютерних систем та моніторинг інформаційних систем.

Для того, щоб впровадити систему моніторингу в діючу інфраструктуру, необхідно врахувати деякі параметри. Система має включати в себе інструменти захисту від несанкціонованого доступу збоку зловмисників (хакерів), безпечну передачу даних, модулі, які дозволяють здійснювати управління мережевим обладнанням, робочими станціями і серверами, як в ручному режимі, так і автономному режимі.

Критерії вибору системи розподіленого моніторингу вимогливі і ним відповідає одна з таких систем – Zabbix. Значна увага при створенні вказаної системи приділяється забезпеченню безпеки цілісності і конфіденційності даних.

Основна задача системи полягає в зборі необхідної інформації, ретельному аналізі та регулярному проведені моніторингу. Окрім розподіленого моніторингу корпоративної мережі, основним завданням постає захист та забезпечення системи, спрямований на підвищення захищеності від несанкціонованого доступу.

Якщо розглянути стан захищеності системи Zabbix, при детальному вивченні можна побачити слабкі та вразливі ланки в програмно-технічному забезпеченні та адмініструванні.

Вищесказане визначає актуальність теми даної бакалаврської роботи,

основний зміст якої становлять дослідження щодо технології забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix.

Об'єкт дослідження – процес забезпечення кібербезпеки інформаційної системи.

Предмет дослідження – методи та засоби забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix.

Мета роботи – розробити рекомендації щодо забезпечення кібербезпеки системи Zabbix із застосуванням двофакторної автентифікації.

Наукові завдання:

дослідити сутність проблеми забезпечення кібербезпеки інформаційних систем;

дослідити сутність завдань забезпечення кібербезпеки інформаційних систем;

проаналізувати існуючі методи та засоби захисту інформаційних систем;

проаналізувати методи та засоби забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix;

проаналізувати основні функції та принципи роботи механізмів забезпечення кібербезпеки системи Zabbix.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання технології забезпечення кібербезпеки системи Zabbix із застосуванням двофакторної автентифікації.

Практичне значення одержаних результатів полягає в розробці варіанту технології забезпечення кібербезпеки системи Zabbix із застосуванням двофакторної автентифікації на основі месенджера Telegram Bot API, а також у розробці рекомендацій щодо застосування технології забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1 Призначення, структура, функції та умови функціонування інформаційних систем

Інформаційна система, яка поєднує в собі апаратне забезпечення, програмне забезпечення, людську силу та процеси, відноситься до мережі, яка використовується для збору, зберігання, обробки, аналізу та розповсюдження даних. Інформаційні системи та професіонали з науковим ступенем у галузі інформаційних систем можуть допомогти підприємствам та іншим організаціям підвищити ефективність, максимізувати прибуток і оптимізувати свою діяльність.

Багато людей вважають інформаційні системи комп'ютерними технологіями. Хоча інформаційні системи часто включають комп'ютери, щоб допомогти керувати даними та досягати бізнес-цілей, вони не обов'язково мають включати комп'ютери.

Існують різні типи інформаційних систем, які можуть служити різним цілям залежно від потреб організації. Приклади:

Сховища даних — це системи керування даними, які підтримують аналітику та інші дії бізнес-аналітики. Вони консолідують і аналізують дані з багатьох джерел. Сховища даних можуть надати інформацію про бізнес, щоб допомогти покращити процес прийняття рішень.

Корпоративні системи, також відомі як системи планування ресурсів підприємства (ERP), — це інтегровані системи, які поєднують усе апаратне та програмне забезпечення, яке використовує бізнес для виконання різних функцій у своїй діяльності. Ці загальноорганізаційні системи допомагають обміну інформацією між відділами та дозволяють інтегрувати процеси з різних частин бізнесу в межах компанії.

Експертні системи використовують штучний інтелект, щоб імітувати прийняття рішень людиною. Програмне забезпечення використовує людські знання для вирішення проблем, які зазвичай потребують досвіду людини. Експертні системи можна застосовувати в таких сферах, як медична діагностика, облік і кодування.

Компоненти інформаційних систем

Кожна інформаційна система включає кілька ключових компонентів: апаратне забезпечення, програмне забезпечення, телекомунікації, людей і дані. Апаратне забезпечення відноситься до фізичних частин інформаційної системи; програмне забезпечення – це програмування, яке керує інформаційною системою; телекомунікаційні передають інформацію через систему; люди керують і взаємодіють з інформаційною системою; а дані — це інформація, яка зберігається в системі та обробляється нею.

Обладнання

Апаратний компонент інформаційної системи містить фізичні елементи системи. Люди можуть торкатися та відчувати частини обладнання. Ці механізми, обладнання та електропроводка забезпечують роботу таких систем, як комп’ютери, смартфони та планшети.

Пристрої введення та виведення є основними елементами технології, які дозволяють людям взаємодіяти з комп’ютерами та іншими інформаційними системами. Прикладами пристроїв введення є клавіатури, миші, мікрофони та сканери. Пристрої виведення можуть включати принтери, монітори, динаміки, звукові та відеокарти.

Апаратні засоби, включаючи мікропроцесори, жорсткі диски, блоки електроживлення та знімні накопичувачі, також дозволяють комп’ютерам зберігати та обробляти дані.

Програмне забезпечення – це нематеріальні програми, які керують функціями інформаційної системи, включаючи введення, виведення, обробку та зберігання.

Системне програмне забезпечення, таке як операційні системи MacOS або Microsoft Windows, є основою для роботи прикладного програмного забезпечення.

Прикладне програмне забезпечення керує програмами, спрямованими на конкретне використання в інформаційних системах. Наприклад, текстові програми використовуються для створення та редагування текстових документів. Програмне забезпечення графічного інтерфейсу користувача (GUI) є одним із найпоширеніших прикладних програм; він представляє інформацію, що зберігається в комп'ютерах, і дозволяє користувачам взаємодіяти з комп'ютерами за допомогою цифрової графіки, наприклад піктограм, кнопок і смуг прокрутки, а не за допомогою текстових команд [8].

Програмне забезпечення може бути відкритим або закритим. Кодування програмного забезпечення з відкритим вихідним кодом є загальнодоступним для користувачів і програмістів, яким вони можуть маніпулювати, тоді як програмне забезпечення із закритим кодом є пропрієтарним.

Телекомунікації

Телекомунікаційні системи з'єднують комп'ютерні мережі та дозволяють передавати через них інформацію. Телекомунікаційні мережі також дозволяють комп'ютерам і службам зберігання отримувати доступ до інформації з хмари.

Існує кілька методів, які телекомунікаційні мережі використовують для передачі інформації. Коаксіальні кабелі та волоконно-оптичні кабелі використовуються операторами телефонного зв'язку, Інтернету та кабельного телебачення для передачі даних, відео та аудіоповідомлень.

Локальні мережі (LAN) з'єднують комп'ютери для створення комп'ютерних мереж у визначеному просторі, наприклад у школі чи вдома. Глобальні мережі (WAN) — це набори локальних мереж, які сприяють обміну даними на великих територіях. Віртуальна приватна мережа (VPN) дозволяє користувачеві захистити свою конфіденційність в Інтернеті шляхом шифрування даних у загальнодоступних мережах.

Мікрохвилі та радіохвилі також можна використовувати для передачі інформації в телекомунікаційних мережах.

Дані

Дані — це нематеріальні необроблені факти, які зберігаються, передаються, аналізуються та обробляються іншими компонентами інформаційних систем. Дані часто зберігаються як числові факти, і вони представляють кількісну або якісну інформацію.

Дані можуть зберігатися в базі даних або сховищі даних у формі, яка найкраще підходить організації, яка їх використовує.

Бази даних містять колекції даних, які можна запитувати або витягувати для певних цілей. Бази даних дозволяють користувачам виконувати фундаментальні операції, такі як зберігання та пошук. З іншого боку, сховища даних зберігають дані з багатьох джерел для аналітичних цілей. Вони дозволяють користувачам оцінювати організацію або її діяльність.

Людські ресурси

Людські ресурси є важливою частиною інформаційних систем. Людський компонент інформаційних систем охоплює кваліфікованих людей, які впливають на дані, програмне забезпечення та процеси в інформаційних системах і маніпулюють ними. Люди, задіяні в інформаційних системах, можуть включати бізнес-аналітики, аналітики інформаційної безпеки або системні аналітики.

Бізнес-аналітики працюють над покращенням операцій і процесів організації. Вони часто зосереджені на підвищенні ефективності та продуктивності або оптимізації розподілу. Аналітики інформаційної безпеки працюють над запобіганням витоку даних і атакам на кібербезпеку. А системні аналітики використовують інформаційні технології, щоб допомогти організаціям оптимізувати роботу користувачів із програмами [7].

Інформаційні системи дозволяють користувачам збирати, зберігати, упорядковувати та поширювати дані — функції, які можуть служити різним цілям компаній. Багато підприємств використовують свої інформаційні системи для управління ресурсами та підвищення ефективності. А деякі покладаються на інформаційні системи, щоб конкурувати на глобальних ринках.

Існує безліч застосувань для різних типів інформаційних систем. Наприклад, ГІС може допомогти дослідникам відстежувати рух морського льоду, сприяти прийняттю рішень щодо сільського господарства або запропонувати розуміння моделей злочинності. Програмне забезпечення електронної пошти, таке як Microsoft Outlook, є поширеним типом системи автоматизації офісу, яка може автоматично сортувати, визначати пріоритети, зберігати та відповідати на повідомлення. A SIRI від Apple — це добре відома експертна система, яка працює, щоб відтворити прийняття рішень людиною за запитами користувачів. Інформаційні системи стають все більш інтегрованими в повсякденне життя, від перегляду Інтернету до онлайн-банкінгу.

На безпеку інформаційної системи істотно впливає той факт, що безпомилкових програм не існує і це стоється не тільки окремих програм, але і цілого ряду програмних продуктів фірм, відомих у всьому світі, наприклад, Microsoft.

Беручи до уваги щодо випадкових загроз з найчастішими та найнебезпечнішими (за збитком) є «людський фактор» − це ненавмисні помилки штатних користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи, за опублікованими даними, у середньому, до 60% інформації безслідно зникає саме через це.

Високі темпи розвитку інформаційних технологій визначають актуальність інформації для її користувачів, інформаційних ресурсів та каналів передачі даних, а також вимагають постійного вдосконалення механізмів захисту інформаційних систем в комплексі. Безпека інформаційних систем є частиною більш широкої проблеми, такої як безпека комп'ютерних систем, або ще більш загальної проблеми - інформаційної безпеки. Можна сказати, що безпека інформаційних систем це захищеність інформації від випадкових або навмисних впливів природного або штучного характеру.

Забезпечення інформаційної безпеки має бути спрямована перш за все на запобігання ризикам, а не на ліквідацію їх наслідків. Саме прийняття запобіжних заходів щодо забезпечення конфіденційності, цілісності, а також доступності

інформації і є найбільш правильним підходом у створенні підсистеми інформаційної безпеки.

Для того, щоб протистояти перерахованим загрозам, сучасні інформаційні системи включають в себе різноманітні системи безпеки, які реалізують політику безпеки. В залежності від цілей і умов функціонування інформаційної системи можуть визначати права доступу суб'єктів до ресурсів, регламентувати порядок аудиту дій користувачів в системі, захисту мережевих комунікацій, створювати способи відновлення системи після випадкових збоїв та інше.

Для реалізації прийнятої політики безпеки існують правові, організаційно-адміністративні та інженерно-технічні, а також заходи захисту інформації.

Правове забезпечення безпеки інформації - це сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, посібників, вимоги яких є обов'язковими в системі захисту інформації.

Інженерно-технічні заходи являють собою сукупність спеціальних органів, технічних засобів і заходів, що функціонують спільно для виконання певного завдання щодо захисту інформації. До інженерних засобів відносять екранування приміщень, організація сигналізації, охорона приміщень з ПК. Вони або запобігають фізичне проникнення, або, якщо проникнення все ж сталося, перешкоджають доступу до даних, в тому числі за допомогою маскування даних. Першу частину завдання забезпечують замки, решітки на вікнах, захисна сигналізація та інші. Другу - генератори шуму, мережеві фільтри, скануючи радіоприймачі і безліч інших пристроїв.

Організаційно-адміністративне забезпечення безпеки інформації є регламентацію виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі таким чином, щоб розголошення, витік і несанкціонований доступ до інформації ставав неможливим або суттєво мав труднощі за рахунок проведення організаційних заходів.

Рішення задач технічного захисту інформації передбачає наявність фахівців в області захисту інформації та оснащення підрозділів спеціальною технікою виявлення і блокування каналів витоку. Вибір спецтехніки для вирішення завдань

технічного захисту інформації визначається на основі аналізу ймовірних загроз і ступеня захищеності об'єкта.

Технічні засоби захисту інформації включають в себе апаратні, програмні, криптографічні засоби захисту, які ускладнюють можливість атаки, допомагають виявити факт її виникнення, позбутися від наслідків атаки, також включають програми для ідентифікації користувачів, контролю доступу, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та інше.

У (табл. 1.1) представлені взаємозв'язок функцій безпеки інформаційних систем і механізмів їх реалізації.

Таблиця 1.1.

Взаємозв'язок функцій безпеки і механізмів їх реалізації

Послуга безпеки	Шифрування	ЕЦП	Мех. управління доступом	Мех. контролю цілісності	Мех. аутентифікації	Мех. доповнення трафіку
Аутентифікація партнерів	+	+			+	
Аутентифікація джерела	+	+				
Управління доступом			+			
Конфіденційність даних	+					+
Цілісність даних	+	+		+		
Належність		+		+		

Важливим завданням сучасних інформаційних систем є забезпечення безпеки інформації, яка в них зберігається та оброблюється. Захист інформації означає забезпечення конфіденційності, цілісності, доступності, автентичності інформації. Існує велика кількість регламентуючих документів, що визначають вимоги до безпеки інформаційних систем і поділяють їх відповідно до виконання цих вимог.

Інформаційні системи схильні до значної кількості загроз. Основними механізмами захисту від цих загроз є шифрування, електронний цифровий підпис, контроль цілісності, доповнення трафіку, механізми управління доступом.

Варто зазначити, що для вирішення питань комплексного захисту інформаційних систем потрібно використовувати, різноманітні рішення, що включає в себе програмно-технічні засоби та інструменти забезпечення інформаційної безпеки та засобів захисту інформації.

Організувати інформаційну безпеку допоможуть спеціалізовані програми, розроблені на основі найсучасніших технологій:

Системи виявлення цільових атак на кінцевих точках мережі(EDR);

Системи реагування та управління інцидентами(IRP);

Системи управління процесами інформаційної безпеки(SGRC);

Системи захисту від витоків конфіденційної інформації(DLP);

Контроль привілейованих користувачів(PUM);

Пошук і виявлення атак(Threat Intelligence);

Системи управління доступ(IdM/IAM);

Захист від DDoS;

SIEM-системи [1].

1.2 Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи

Безпека кінцевих точок — це практика захисту кінцевих точок або точок входу пристроїв кінцевих користувачів, таких як настільні ПК, ноутбуки та мобільні пристрої, від використання зловмисниками та кампаніями. Системи безпеки кінцевих точок захищають ці кінцеві точки в мережі або в хмарі від загроз кібербезпеці. Безпека кінцевих точок еволюціонувала від традиційного антивірусного програмного забезпечення до комплексного захисту від складних зловмисних програм і нових загроз нульового дня.

Організації будь-якого розміру піддаються ризику з боку національних держав, хактивістів, організованої злочинності, а також зловмисних і випадкових внутрішніх загроз. Безпека кінцевих точок часто розглядається як головна лінія

кібербезпеки, і це одне з перших місць, де організації прагнуть захистити свої корпоративні мережі.

Оскільки обсяг і складність загроз кібербезпеці неухильно зростають, зростає потреба в більш досконалих рішеннях безпеки кінцевих точок. Сучасні системи захисту кінцевих точок розроблені для швидкого виявлення, аналізу, блокування та стримування поточних атак. Для цього вони повинні співпрацювати один з одним та з іншими технологіями безпеки, щоб надати адміністраторам бачення передових загроз, щоб пришвидшити час виявлення та реагування на виправлення.

Платформа захисту кінцевої точки є важливою частиною кібербезпеки підприємства з кількох причин. Перш за все, у сучасному діловому світі дані є найціннішим активом компанії, і втрата цих даних або доступу до них може поставити весь бізнес під загрозу банкрутства. Підприємствам також доводиться стикатися не лише зі зростанням кількості кінцевих точок, але й із збільшенням кількості типів кінцевих точок. Ці фактори самі по собі ускладнюють безпеку кінцевої точки підприємства, але вони ускладнюються політиками віддаленої роботи та BYOD, які роблять захист периметра дедалі недостатніми і створюють уразливості. Ландшафт загроз також ускладнюється: хакери завжди винаходять нові способи отримати доступ, викрасти інформацію або змусити співробітників надати конфіденційну інформацію. Якщо додати до цього можливість, вартість перерозподілу ресурсів із бізнес-цілей на боротьбу із загрозами, репутаційні витрати від масштабного порушення та фактичні фінансові витрати від порушень відповідності, і легко зрозуміти, чому платформи захисту кінцевих точок стали вважатися обов’язковими. має з точки зору забезпечення сучасних підприємств.

Серед найпоширеніших ризиків безпеки кінцевих точок:

Фішинг

Найбільш популярною та найменш складною формою атаки, фішингом, є використання фальшивих повідомлень для отримання доступу. Повідомлення нібито надходить від надійної організації (наприклад, банку чи відомої компанії), щоб оманою змусити користувачів надати особисту інформацію або завантажити зловмисне програмне забезпечення. Далі інформація або зловмисне програмне

забезпечення використовуються для отримання доступу до системи користувача, а звідти – закріплення у більшій мережі, у якій працює користувач.

Застарілі патчі

Одна з проблем сучасного життя: постійні виправлення — це невелика незручність, але необхідне зло, щоб не відставати від нових загроз в Інтернеті. І все ж багато компаній (навіть ті, що входять до списку Forbes 500) досі нехтують натисканням кнопки оновлення.

Реклама шкідливих програм

Ця афера, також відома як шкідлива реклама, використовує легітимну рекламу та може поширюватися на авторитетних веб-сайтах і в соціальних мережах, перш ніж її буде видалено.

В останні роки з'явилися складні шкідливі програми, які взагалі не вимагають жодної взаємодії з користувачем. Таке зловмисне програмне забезпечення перед клацанням можна вбудовувати в основні сценарії веб-сторінок, дозволяючи їм запускатися автоматично, навіть без натискання користувачем.

Drive-by Download

Подібно до фішингу, цей метод використовує обман, щоб змусити користувачів натиснути посилання або завантажити зловмисне програмне забезпечення. Приклади включають фальшиві системні сповіщення, антивірусні сповіщення або оманливі угоди про встановлення, що відрізняються від програми, яку користувач мав намір завантажити.

Програми-вимагачі

Жоден інший ризик кібербезпеки кінцевої точки не є таким простим вимаганням, як програми-вимагачі. Цей тип зловмисного програмного забезпечення шифрує всі файли користувачів, роблячи їх недоступними, якщо не буде сплачено викуп.

У більшості випадків програма маскується під законну програму, яка обманом спонукає користувачів запустити її, однак з'явилися новіші версії, які не вимагають взаємодії з користувачем і можуть автоматично переміщатися між комп'ютерами в мережі.

DDoS

Розподілена атака на відмову в обслуговуванні використовує потік вхідного трафіку, щоб перевантажити веб-сайт, сервер або мережу. Він використовує скомпрометовані пристрої для неодноразового доступу до цільового сайту та зрештою порушує його пропускну здатність, що призводить до відмови в обслуговуванні звичайного трафіку.

Розширені стійкі загрози

APT відносяться до груп, які отримують доступ до мережі та залишаються непоміченими протягом тривалого часу. Як випливає з назви, вони відрізняються від типових хакерських груп трьома способами:

Розширені – вони мають доступ до широкого спектру як комерційних, так і некомерційних технологій проникнення, включно з розширеним обладнанням і програмним забезпеченням, доступним лише для суб’єктів національної держави.

Стійкі – замість того, щоб бути короткостроковими, APT задоволені тим, що залишаються бездіяльними у скомпрометованих мережах протягом місяців або років, подібно до «сплячих клітинок».

Організовані – порівняно з неформальними групами, APT є високоорганізованими, дисциплінованими та скоординованими у своєму втручанні та виконанні

Отже, висока актуальність атак, пов'язаних з наявністю вразливостей в операційній системі і прикладному програмному забезпеченні, викликана розвитком IT-інфраструктури і неефективними внутрішніми процесами управління уразливими [4].

1.3 Мета та завдання захисту кінцевих точок корпоративної інформаційної системи

Для сучасних інформаційних систем забезпечення безпеки - це складна і багатовекторна задача. Одне з ключових її напрямків - захист мережевого

обладнання, серверів, робочих станцій та кінцевих пристроїв, які є верхівкою інформаційного айсбергу IT-інфраструктури.

Сучасні організації не тільки прагнуть забезпечити співробітників продуктивними робочими місцями, а й надають можливості для віддаленої і мобільної роботи, спрощують доступ до корпоративних ресурсів і додатків. Пристрої, на яких працюють співробітники, часто містять важливі дані і конфіденційну інформацію, і при цьому можуть регулярно використовуватися за межами захищеної корпоративної мережі. Комп'ютери співробітників таким чином стають вразливою ланкою системи інформаційної безпеки організації. При цьому різноманітність платформ вимагає спеціальних підходів для забезпечення безпеки кожного типу пристроїв.

Поширення так званих спрямованих атак (APT - Advanced Persistent Threats), повернуло завдання захисту кінцевих точок в розряд пріоритетних у стратегії забезпечення корпоративної інформаційної безпеки. При подібних атаках саме кінцеві точки найчастіше стають первинними цілями зловмисників. До вразливості прикладного і системного ПО додається людський фактор: стаючи жертвами соціальної інженерії, користувачі самі запускають шкідливі файли або переходять за підробленими посиланнями на заражені ресурси.

Захист кінцевих точок покликана мінімізувати не тільки ймовірність зараження шкідливим кодом, але і несанкціонованих дій з даними, атак на канал передачі інформації між централізованими ресурсами і кінцевою точкою, авторизації зловмисника під іменем легітимного користувача та інші. Для захисту від перерахованих загроз застосовуються механізми автентифікації, засоби захисту каналу і даних, засоби фільтрації веб-контенту, персональний міжмережевий екран та інші інструменти безпеки.

Для підвищення рівня захищеності, при спробі вирішити проблему безпеки інформаційних систем, співробітники IT-відділів намагаються поза комплексом заходів інформаційної безпеки забезпечити захист кінцевих точок від безліч конкретних загроз, встановлюючи на них велике число незалежних агентів: антивірусний захист, IPS-системи, засобів управління оновленнями, систем

шифрування та інше. З часом це призводить до того, що робочі станції навантажуються різними засобами захисту, число яких може досягати десятка. Нерідко конфліктуючи між собою вони не працюють як єдина система і вимагають окремих серверів управління, налаштувань профілів і політик, своєчасного оновлення, що є суттєвим навантаженням на адміністративні та обчислювальні ресурси. А їх одночасна робота може призводити до колізій і знижувати стабільність функціонування додатків операційної системи та активно споживати ресурси кінцевої точки [4].

Тому слід використовувати комплексний підхід, який забезпечує всебічний захист кінцевих точок, що функціонують як єдина система з єдиним програмним модулем і об'єднує різні компоненти безпеки. Така уніфікація дозволяє домогтись максимальної захищеності при одночасній оптимізації витрат. При виборі рішення необхідно переконатися, що воно відповідає вимогам стандартів безпеки, застосовує заходи безпеки більшості відомих загроз, прозоро для користувачів і має можливість централізованого керування.

Побудова корпоративної системи повинна починатися з інформаційної безпеки та забезпечення захисту кінцевих точок, які завжди були якщо не головним, то одним з основних джерел загроз інформаційній безпеці. Слід зазначити, що на кінцевих точках ведеться обробка великого обсягу даних, в тому числі з впливом людського фактору, тому слід підходити до комплексного і централізованого вирішення цього питання, що обумовлює відповідну увагу до ІБ кінцевих пристроїв.

Зростаюча складність загроз призводить до того, що традиційні методи захисту стають неефективними. Стандартних засобів захисту недостатньо, щоб виключити витік даних або проникнення зловмисників в мережу, а установка декількох вузькоспеціалізованих рішень часто призводить до конфліктів і помилок. До того ж налаштування і супровід спільної роботи декількох захисних програм - завдання не з легких. Потрібно комплексне рішення, яке дозволить користувачам з комфортом виконувати свої робочі функції, але при цьому забезпечить збереження інформаційних активів компанії.

Безпека кінцевих точок — це багаторівнева ініціатива, спрямована на блокування загроз і безпеку кінцевих точок мережі. Рішення для кінцевих точок працюють із централізованим програмним забезпеченням із встановленням на кожному пристрої. Платформи кінцевих точок відображають більші системи з міжмережевими екранами, контролем доступу та оцінкою вразливості для нейтралізації загроз.

Усі рішення безпеки кінцевих точок повинні забезпечувати класифікацію даних і запобігання втратам, моніторинг внутрішніх загроз, контроль доступу до мережі та привілейованих користувачів, захист від зловмисного програмного забезпечення, шлюзи електронної пошти та відповідь на виявлення кінцевих точок (EDR).

Крім того, шифрування та контроль програм відіграють важливу роль у безпеці кінцевої точки. Шифрування має важливе значення для забезпечення захисту даних у спілкуванні. Контроль додатків запобігає ризикованому використанню кінцевих додатків, до чого схильні люди. Безпека кінцевої точки використовує певні методи для блокування загроз і захисту мережі. Ось деякі з них, про які варто пам’ятати:

Шифрування: передбачає кодування та шифрування даних, що робить їх нерозбірливими без ключа. Шифрування є останнім і, можливо, найважливішим рівнем безпеки, оскільки воно захищає дані, навіть якщо вони потрапляють у чужі руки.

Криміналістичний аналіз: працює в поєднанні з EDR, відстежуючи всі дії кінцевих точок і створюючи цифровий відбиток усіх інцидентів. Уся інформація та докази щодо атаки — що сталося, хто несе відповідальність і наслідки — збираються та аналізуються, щоб запобігти інцидентам у майбутньому.

Захист IoT: багатьом пристроям IoT дуже бракує належного захисту після встановлення. Розпочати слід зі становлення системи EDR для керування, моніторингу та сканування вразливостей. Обов’язкове видалення застарілих пристроїв, встановлення рішення нового покоління, відстежування всіх програм та

доступ до пристроїв, шифрування зв’язку і сегментування мережі, щоб ізолювати проблеми.

Шлюзи електронної пошти. Електронна пошта є найпоширенішим способом атаки злочинців на мережі, тому програмне забезпечення шлюзу електронної пошти сьогодні є критично важливим. Безпечні електронні листи залишаються в системі, тоді як потенційні загрози відправляються в карантин. Усі шлюзи електронної пошти повинні включати блокування вірусів і шкідливих програм, фільтрацію вмісту та архівування електронної пошти.

Карантин: це практика розділення небезпечних файлів, щоб запобігти пошкодженню пристроїв і мереж. Швидка ізоляція небезпечних файлів є важливою для безпеки кінцевої точки, а карантин також дозволяє очищати цінні файли, а не викидати їх.

Як правило, програмне забезпечення безпеки кінцевої точки включає в себе такі ключові компоненти:

Використання машинного навчання для виявлення загроз нульового дня майже в реальному часі

Розширений захист від зловмисного програмного забезпечення та антивірусний захист для захисту, виявлення та виправлення зловмисного програмного забезпечення на кількох кінцевих пристроях і операційних системах

Проактивна веб-безпека для безпечного перегляду веб-сторінок

Класифікація даних і запобігання витоку даних для запобігання втраті та ексфільтрації даних

Інтегрований брандмауер для блокування ворожих мережевих атак

Шлюз електронної пошти для блокування спроб фішингу та соціальної інженерії, націлених на ваших співробітників

Криміналістична експертиза загроз, що дозволяє адміністраторам швидко ізолювати інфекції

Захист від внутрішніх загроз для захисту від ненавмисних і зловмисних дій

Централізована платформа керування кінцевими точками для покращення видимості та спрощення операцій

Шифрування кінцевої точки, електронної пошти та диска для запобігання викраданню даних [3].

Отже, сучасні технологічні продукти для захисту кінцевих точок повинні бути комплексними, багатоярусними системами та розвиватися швидше супротивників і блокувати загрози ще до того, як вони потраплять в захищену інформаційну систему.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ РОЗПОДІЛЕНОГО МОНІТОРИНГУ СТАНУ КОРПОРАТИВНОЇ МЕРЕЖІ ZABBIX

2.1 Аналіз існуючих методів та засобів захисту кінцевих точок корпоративної інформаційної системи

Технології захисту кінцевих точок за останні 25 років значно змінилися. Раніше єдиними проблемами були віруси і спам. Однак швидке зростання економіки кіберзлочинністю світу, постійно мінливий IT-ландшафт і ризиковану поведінку користувачів призвели до експоненціального зростання витончених загроз, таких як фішинг, цільові атаки, шкідливі програми для мобільних пристроїв і програми-вимагачі.

Велика різноманіття векторів атак на кінцеві точки, в свою чергу, породжує і великий "парк" технічних засобів захисту, що призводить до гострої потреби в розстановці пріоритетів при виборі технологій цих засобів і загальному проектуванні системи в цілому.

На сьогодні в багатьох організацій серйозно ставляться щодо питань інформаційного захисту, та висувають широкий ряд вимог до сучасних систем безпеки. Якщо раніше всі вимоги зводилися лише до якості роботи антивіруса, то сьогодні ситуація змінилася. При великій різноманітності шкідливих додатків, і зростанні складності інформаційних систем, що потребують захисту, основними вимогами стали: кроссплатформенність системи захисту і тотальний контроль за всіма типами додатків, що запускаються на корпоративних комп'ютерах.

В цей час актуальнішим стає питання перегляду технологій захисту кінцевих точок, оскільки традиційних засобів вже стає недостатньо для протидії сучасним кіберзагрозам. Щоб уберегти свої дані та інфраструктуру від все більш складних загроз компанії повинні використовувати багаторівневі ешелоновані рішення.

При вирішенні цього завдання, як і раніше важливу роль відіграють системи для захисту кінцевих точок. Не секрет, що деякі підприємства покладаються для

досягнення захисту на вбудований в операційну систему Windows Defender. Однак його можливостей недостатньо, щоб запобігти від кіберзагроз. Адже є сучасніші, та якісні комплекси захисту класу Endpoint Protection Plarform (EPP), які забезпечують набагато більш повний та надійний захист на кожній фазі атаки, і призначений для більш ефективного захисту від цілеспрямованих кібератак та реагування на які виявляються інциденти інформаційної безпеки.

Більше того, дотримання політик безпеки класу EPP-рішень з урахуванням зростаючого числа загроз сьогодні вимагає використовувати як мінімум:

Файрволи для різних типів пристроїв;

Антивіруси для електронної пошти;

Моніторинг, фільтрацію і захист веб-трафіку;

Управління безпекою і захисні рішення для мобільних пристроїв;

Контроль роботи додатків;

Шифрування даних;

Засоби виявлення вторгнень.

При цьому ринок пропонує три основні рішення захисту кінцевих пристроїв та їх комбінації:

1. Традиційні антивіруси, засновані на сигнатурах. Дають стабільний результат – але лише в межах бази сигнатур. В силу неймовірно великої кількості шкідливих зразків вона не може бути актуальною на 100% в кожен момент часу, плюс користувач здатний відключити антивірус на своїй машині.

2. Endpoint Detection and Response (EDR) або виявлення і реагування на інциденти. Такі рішення розпізнають індикатор компрометації на кінцевому пристрої і блокують і / або лікують його. Зазвичай ці системи працюють тільки за фактом злому (вторгнення) на пристрій або в корпоративну мережу.

3. Advanced Endpoint Protection (AEP) або просунуту захист кінцевих пристроїв, яка включає превентивні методи захисту від експлойтів і шкідливого ПО, контроль пристроїв і портів, персональні файрволи та так далі. Тобто AЄP-рішення бореться з погрозами: загроза розпізнається і знищується ще до злому, як,

наприклад, в Palo Alto Networks Traps, Check Point SandBlast Agent (це рішення при виявленні підозрілих активностей робить резервні копії) або Forticlient.

Якщо дати точне визначення EPP – це рішення, розгорнуте на кінцевих пристроях, для запобігання атак на основі файлів, виявлення шкідливих дій і забезпечення розслідування і відповідної реакції, необхідних для реагування на динамічні інциденти безпеки і попередження про них.

Цей клас EPP-рішень є прямим нащадком перших антивірусів. І якщо раніше антивірусні виробники боролися в основному за повноту і обсяг сигнатурних баз, то сьогодні боротьба розгортається вже за зручність користування, вбудовані механізми самозахисту і стійкість до технікам обходу і новим загрозам. Відмінною особливістю таких систем є наявність як корпоративних рішень з виділеної системою управління і звітності, так і рішень для захисту домашніх комп'ютерів користувачів і мобільних пристроїв, з підтримкою практично всієї Enterprise-функціональності.

Розширення функціональності (Next Generation Firewall) NGFW на кінцеві станції користувачів в рамках комплексного підходу до забезпечення мережевої безпеки виробники NGFW були змушені створювати рішення для захисту кінцевих станцій, щоб забезпечити більшу видимість і не допустити розмиття периметра безпеки, особливо в організаціях, що використовують (bring your own device) BYOD-підхід. Маючи значний досвід комплексної мережевої безпеки, виробники NGFW випускають досить конкурентні рішення, багато з яких можна назвати NGEPP. Зазвичай рішення таких виробників представлені виключно в корпоративному сегменті.

При впровадженні сучасних рішень для ефективного захисту робочих станцій і серверів, в першу чергу слід звертати увагу на їхню здатність запобігати зараженню на кожному етапі. Також крім високоточного детектування сучасних загроз, комплекс Endpoint Protection Plarform повинен відповідати таким вимогам як низьке навантаження кінцевих точок і легке управління.

Таким чином, захист станцій вимагає комплексного підходу, що включає всі перераховані етапи: запобігання, передове виявлення, реагування, усунення

наслідків атак і розслідування. Забезпечити таку функціональність дозволяє спільна експлуатація рішень класу EPP і EDR.

EPP (Endpoint Protection Platform) - клас рішень, призначений для запобігання і блокування відомих загроз, виявлення шкідливої активності. Комплексний захист робочої станції, що включає класичний антивірус, розширені технології безпеки (персональний міжмережевий екран, система запобігання вторгнень, контроль додатків, управління зйомними носіями та інші) і інструменти розслідування та відновлення.

Традиційні рішення класу EPP справляються з відомими погрозами, але нові і незвичайні вектори атак інколи здатні їх заплутати. Зокрема, вони не мають ефективних інструментів для аналізу атак і не можуть визначити, що окремі зафіксовані в логах інциденти – це частина комплексної кібератаки на інфраструктуру, а безфайлові віруси можуть просто не помітити. Ці рішення успішно справляються з фіксацією інцидентів на окремих пристроях, але, як правило, не в змозі виявити, що ці інциденти є фрагментами складної комплексної атаки, яка в перспективі здатна нанести організації серйозної шкоди. Можливості автоматичного аналізу інцидентів у них майже відсутні. Тому компанії розробили рішення класу EDR (Endpoint Detection and Response).

Треба зазначити, що сучасній EPP відводиться і роль EDR-системи з класичними ознаками таких систем, як розслідування інциденту і можливістю формування реакції на нього. Необхідно пам'ятати, що EDR-системи як клас з'явилися якраз з припущення, що неможливо запобігти 100% атак на кінцеві станції, і необхідності мати можливість досліджувати інцидент і виходячи з цього сформувати відповідну реакцію. Саме тому EDR в майбутньому повинен стати невід'ємною частиною будь-якого EPP-рішення, що претендує на звання Next Generation Endpoint Protection Platform.

EDR (Endpoint Detection and Response) – це більш сучасний клас рішень, призначений для виявлення і реагування на просунуті загрози. Оперативно виявляє відхилення в поведінці додатків і об'єктів з можливістю їх швидкого відновлення в разі підтвердження інциденту співробітником ІБ. Їх головна перевага - це

поєднання класичних інструментів з арсеналу EPP і ефективної системи аналізу, виявлення та попередження атак (включаючи і так звані «атаки нульового дня»). Завдяки застосуванню нових технологій, а також інтелектуального відстеження та фіксації всієї активності системи і її компонентів, рішення EDR набагато частіше виявляють і знешкоджують комплексні кіберзагрози і атаки без використання «прямих» методів, наприклад, безфайлові атаки. При цьому системи EDR не спираються на сигнатури або чорні списки [6].

Ринок EDR зараз тільки починає формуватися і має хороші перспективи для подальшого розвитку. Перший досвід впровадження рішень класу EDR продемонстрував їх високу ефективність і здатність реально підвищити рівень захисту, в тому числі і від цілеспрямованих атак зловмисників.

Зазвичай рішення EDR виступають як самостійний продукт, або як частина платформи Anti-APT, інтегруючись з пісочницями і забезпечуючи більш високий рівень детектування підозрілої активності та можливість активного реагування на інциденти. Але сьогодні вже неможливо уявити інфраструктуру великої компанії без SIEM-системи, тому що, Security Operation Center є одним з основних робочих інструментів співробітника безпеки. EDR можуть істотно збагатити інформацією SIEM-систему, надаючи додаткові можливості для моніторингу і проведення розслідувань.

З точки зору корпоративної системи захисту EDR є додатковим елементом безпеки, який дозволяє виявляти дії зловмисника, коли він вже зміг подолати всі наявні засоби захисту. Крім того, EDR дозволяють за допомогою виявлення аномалій виявити підозрілі файли і направити їх на дослідження в «пісочницю» - віртуальне середовище, використовувану антивірусними аналітиками для виявлення шкідливої активності кодів і додатків. Саме тому зараз виробники антивірусних рішень з одного боку і розробники мережевих засобів захисту з іншого намагаються вмонтувати функції EDR в свої продукти.

Таким чином, EDR по суті доповнює встановлену EPP, розширюючи можливості щодо захисту кінцевих пристроїв. При цьому рішення класу EPP забезпечують захист від відомих типів атак, а EDR – інші етапи життєвого циклу

інциденту: детектування, реагування та розслідування, а часто і функції по аналізу ефективності роботи EPP для виявлення слабких місць в захисті. На сьогодні спостерігається зближення цих систем - в EDR-платформах з'являється функціонал EPP і навпаки.

Основні функціональні можливості рішень із захисту кінцевих точок класу EPP і EDR:

Запобігання – блокування загальних загроз та захист основних систем для зниження ризику просунутих загроз. Рішення включають в себе не тільки антивірусні технології, але і технології репутації, поведінкового аналізу, управління додатками і пристроями, що дозволяє блокувати загрози найефективнішим способом. Даний функціонал реалізований в рішеннях класу EPP.

Сучасне виявлення – постійний моніторинг, дослідження та виявлення просунутих загроз. Рішення дозволяють шукати свідоцтва злому в усій мережі в режимі реального часу, зіставляти попередження, що надходять із засобів управління мережевою безпекою, з подіями на робочих місцях в режимі реального часу. Для цього використовуються комбінації різних механізмів і методів детектування, таких як статичний аналіз, машинне навчання, ретроспективний аналіз та інше. Даний функціонал реалізований в рішеннях класу EDR.

Реагування – управління інцидентом і оперативна нейтралізація атаки для пом'якшення наслідків. Рішення поєднують технології передового виявлення і реагування, що дозволяє скоротити час життя загроз з декількох днів або тижнів до лічених хвилин. Оперативне реагування на інциденти забезпечується за рахунок кореляції тисяч подій з наступним виділенням найбільш підозрілих. Відповідні заходи можуть включати зупинку процесу на хості, заборона запуску виконуваного файлу, віддалену модифікацію реєстру і ізоляцію хоста. Оперативна візуалізація повного ланцюжка інциденту, реагування і зупинка атаки займають кілька хвилин, що є запорукою пом'якшення наслідків загроз. Даний функціонал реалізований в рішеннях класу EDR.

Усунення наслідків – повне видалення інфекції та її слідів з мінімальним впливом на кінцевих користувачів. Рішення включають інструментарій щодо усунення наслідків загроз і дозволяють скасувати зміни, внесені шкідливим програмним забезпеченням. У цьому випадку файли і реєстр повертаються в первинний стан.

Розслідування – швидкий збір і аналіз інформації, оперативне вжиття заходів. Рішення містять інструментом комплексного оперативного розслідування та глибокого аналізу цільової атаки. Дані платформи дозволяють аналітикам, ІБ-офіцерам, співробітникам SOC і центрам реагування швидко зібрати і проаналізувати інформацію в автоматичному або ручному режимах і оперативне вжити заходів. Важливо враховувати, що ручний розбір інциденту займає тривалий час і може негативно позначитися на бізнес-процесах при втручанні аналітика в роботу хоста.

Тут також можна зазначити додаткові функціональні інструменти EPP і EDR, дають величезну перевагу над простими рішеннями захисту кінцевих пристроїв:

Захист від шифрувальників.

Для боротьби з такими видами загроз виробники застосовують комплекс заходів, що включає і поведінковий аналіз, і машинне навчання. Наприклад, рішення виявляють і завершують процеси, які намагаються маніпулювати тіньовими копіями, головного завантажувального блоку, певним набором контрольованих файлів на кінцевій точці. При цьому деякі продукти дозволяють проактивно створювати короткострокові бекапи "на ходу" і відновлювати зашифровані файли.

На тлі великої кількості атак вірусів-шифрувальників даний кейс як один із драйверів зростання популярності теми захисту кінцевих станцій ми винесли в окремий блок. WannaCry і Petya - яскраві приклади швидко поширюється хробака і деструктивного вірусу-здирника.

Відповідність вимогам.

Рішення дозволяють організаціям досягти відповідності стандартам, необхідним великими регулюючими органами, наприклад, PCI DSS. В основі

відповідності лежать здатність постійного моніторингу активів, відстеження та застосування політик управління змінами, можливість аудиту.

Інтеграція.

Наявність API дозволяє проводити інтеграцію системи і сторонніх рішень. Наприклад, частина рішень реалізують перевірку підозрілих об'єктів з хостів в "пісочниці" з отриманням відповідного вердикту / зворотного зв'язку.

Увесь додатковий функціонал входить в базові можливості деяких EPP-рішень, а також реалізований в EDR. Можливо перетин деяких функцій з EPP і EDR-рішень.

Розгорнуте рішення класу EDR може бути доповнено службою MDR (Managed Detection & Response), тобто послугою може знаходити загроз і реагуванням на них. В рамках сервісу MDR використовуються підходи проактивного виявлення загроз (cyber threat hunting), а також здійснюється первинне реагування на інциденти безпеки. В MDR входить обробка пов'язаних з інформаційною безпекою подій IT-інфраструктури, що робить його схожим на роботу центру щодо забезпечення безпеки (SOC - Security Operation Center). Основні відмінності – типи подій, які виявляються при про активному пошуку невідомих загроз, досвід і рівень знань фахівців в області пошуку загроз, а також доступ до глобальної базі даних про загрози (Threat Intelligence). Такі служби найчастіше працюють "за підпискою" і займаються моніторингом безпеки замовника в цілодобовому режимі. Вони дозволяють знизити навантаження на IT-спеціалістів компаній, взявши на себе аналіз подій, відсіювання помилкових спрацьовувань і розстановку пріоритетів при отриманні нових даних, виявлення потенційних загроз і автоматичний підбір інструментів для захисту від них. Ці ж служби допомагають сформувати плани заходів щодо усунення загроз і запобігання повторних атак, що особливо важливо для компаній з недоукомплектованим або мінімальним штатом фахівців з інформаційної безпеки.

Важливим зрушенням на міжнародному ринку EPP-рішень по захисту кінцевих станцій є рух від реактивної захисту за допомогою IoC (Indicators of Compromise), які активно використовуються існуючими EPP-рішеннями (особливо

з яскраво вираженою EDR-функціональністю), в сторону проактивного захисту за допомогою IoA (Indicators of Attack), використання яких дозволяє в реальному часі боротися зі складними спрямованими атаками. Безумовно, при русі від IoC-підходу, який близький до класичного сигнатурному аналізу, в сторону IoA-підходу виробники NGEPP використовують сучасні технології визначення атак, засновані в тому числі на технологіях поведінкової аналітики, машинного навчання і нейронних мережах. Ще одним важливим відмінністю сучасних NGEPP є кількість підтримуваних платформ, починаючи від десктопних Windows і macOS, закінчуючи Open Source і мобільними рішеннями. На сьогодні в стандартні пакети практично будь-якого NGEPP-рішення включаються функції по управлінню безпекою мобільних пристроїв, які мають безліч перетинів з функціональністю спеціалізованих MDM-систем (Mobile Device Management).

Тим не менш, обмежуючись таким широким визначенням EPP, можна випустити з уваги дійсно ефективні рішення для захисту кінцевих станцій, просто тому, що якийсь із перерахованих вище ознак ще не реалізований повною мірою. Тому при розгляді все EPP-системи пропонується розділити на три еволюційних класу:

1. Розвиток класичних антивірусних рішень.

Цей клас EPP-рішень є прямим нащадком перших антивірусів. І якщо раніше антивірусні виробники боролися в основному за повноту і обсяг сигнатурних баз, то сьогодні боротьба розгортається вже за зручність користування, вбудовані механізми самозахисту і стійкість до технікам обходу і новим загрозам. Відмінною особливістю таких систем є наявність як корпоративних рішень з виділеної системою управління і звітності, так і рішень для захисту домашніх комп'ютерів користувачів і мобільних пристроїв, з підтримкою практично всієї Enterprise-функціональності. До представників цього класу EPP-рішень можна віднести: Kaspersky Endpoint Security, TrendMicro Smart Protection Suites, ESET Endpoint Protection, Symantec Endpoint Protection, Dr.Web Enterprise Security Suite та інші.

2. Розширення функціональності NGFW (Next Generation Firewall) на кінцеві станції користувачів.

В рамках комплексного підходу до забезпечення мережевої безпеки виробники NGFW були змушені створювати рішення для захисту кінцевих станцій, щоб забезпечити більшу видимість і не допустити розмиття периметра безпеки, особливо в організаціях, що використовують BYOD-підхід.

Маючи значний досвід в комплексній мережевої безпеки, виробники NGFW випускають досить конкурентні рішення, багато з яких по праву можна назвати NGEPP.

Зазвичай рішення таких виробників представлені виключно в корпоративному сегменті. До найвідоміших представників цього класу EPP-рішень можна віднести: Check Point Endpoint Security, Fortinet FortiClient, Palo Alto Networks Traps і інші.

3. Окремі рішення, які використовують екзотичні та унікальні підходи до забезпечення безпеки кінцевих станцій.

Класичний підхід інтеграції багатьох функцій захисту кінцевих станцій в одному продукті не завжди є єдино можливим. На доказ цього на ринку EPP стали з'являтися рішення, які виходять за рамки класичної парадигми захисту кінцевих станцій, але при цьому можуть скласти конкуренцію піонерам цього ринку.

Яскравим прикладом таких систем можна вважати CylancePROTECT, який використовує алгоритми машинного навчання для боротьби з відомими і невідомими погрозами, при цьому не вимагаючи регулярних оновлень і не використовуючи сигнатурний підхід. Ще один приклад нестандартного підходу – BufferZone, що відповідає тільки за контейнерування (запуск в ізольованому системному оточенні) всіх недовірених додатків, таким чином захищаючи системні файли і критичні дані без як такого аналізу активності додатків.

В ідеальній ситуації, всі ці інструменти для зручності клієнтів об'єднуються в один програмний комплекс, який здатний працювати з будь-якими платформами, реагувати на виявлені загрози без участі користувачів, використовувати поведінковий аналіз і виявляти нові типи загроз. Також подібні комплекси сильно полегшують роботу IT-фахівцям і набагато краще захищають корпоративні мережі

від користувачів, які не дуже замислюються про те, які програми скачують і які сайти відвідують в робочий час [2].

2.2 Призначення, основні функції та склад засобів забезпечення кібербезпеки системи Zabbix

Автоматизовані системи моніторингу грають важливу роль в житті сучасного суспільства. Моніторинг – це безперервний процес спостереження і реєстрації параметрів об'єкта в порівнянні з заданими критеріями [26]. У ряді галузей дані збираються і накопичуються дуже інтенсивно. Через тенденції зростання мереж передачі даних підвищуються вимоги до систем моніторингу цих мереж. Враховуючи сучасний стан інформаційних і комунікаційних технологій для концентрації інформації щодо комп’ютерних мереж постає проблема моніторингу.

Однією з найважливіших частин інформаційної інфраструктури сучасних підприємств, приватних компаній і багатьох державних організацій є корпоративні мережі передачі даних, які давно перейшли в розряд критичних для забезпечення бізнес-процесів.

Корпоративні мережі мають високу складність в силу територіальної розподіленої інфраструктури, поєднання можливостей власне передачі даних з використанням телефонії та відео конференц-зв'язку, наявності вбудованих систем підтримки інформаційної безпеки, а також резервних і дублюючих елементів, що відповідають за забезпечення надійності та доступності корпоративної мережі. В таких умовах гостро стоїть проблема підтримки параметрів роботи мережі на заданому рівні, що є нетривіальним завданням [10].

В першу чергу тут необхідна підтримка мережевої інфраструктури. Вона вимагає великого штату кваліфікованих фахівців, в обов'язки яких входить підтримка доступності мережевих сервісів, оптимізація роботи мережі, налагодження та оновлення мережевого апаратного і програмного забезпечення, виявлення і усунення виникаючих інцидентів, грамотна технічна підтримка та інші аналогічні функції. Крім цього не виключені труднощі в процесі експлуатації

системи. При розширенні мережі збільшується і кількість складових її об'єктів, які потребують моніторингу, а отже, і навантаження на систему моніторингу. Крім того, при традиційному обслуговуванні мереж всі дії по усуненню несправностей або "вузьких місць" виконуються post factum, уже після того, як виникли негативні наслідки. Необхідно відзначити, що ці ж проблеми виникають і в великих комерційних компаніях. Така ситуація спричиняє за собою уповільнення реакції на аварійні події в мережі, веде до деградації мережевих сервісів і служб.

Для вирішення більшої частини описаних проблем та запобігання цим ситуаціям використовуються системи моніторингу та управління мережею. Цей клас завдань забезпечує інвентаризацію і розширену діагностику комп'ютерних мереж, містить:

постійний контроль функціонування використовуваного мережевого обладнання, прикладних систем і мережевих сервісів;

збір статистики (в реальному часі і в вигляді архівів) і візуалізацію ключових показників продуктивності і операційних параметрів мережевої інфраструктури;

оптимізацію навантаження на мережеве обладнання та сервери;

фіксацію інцидентів;

аналіз впливу виявлених несправностей;

локалізацію причин інциденту і його автоматичне усунення, або повідомлення відповідальних за його усунення осіб.

Система моніторингу – це потужний засіб підтримки і аналізу стану мережевих ресурсів, що дозволяє забезпечувати цілодобовий контроль за мережевими ресурсами масового користування. Вона також забезпечує оповіщення про критичний стан ресурсів, що дозволяє негайно вжити заходів для підтримки роботи цих ресурсів.

Використання подібних систем дозволяє організації здійснювати проактивний моніторинг доступності, стану і продуктивності компонент корпоративної / відомчої мережі передачі даних, аналізувати і оптимізувати їх завантаження, а також прогнозувати виникнення позаштатних ситуацій. Це дає можливість значно скоротити число критичних збоїв і знизити навантаження на

персонал організації. Дрібні збої, що становлять основну масу інцидентів, за допомогою систем моніторингу та управління мережею виправляються або автоматично, або за допомогою віддаленого адміністратора. Що стосується великих інцидентів, то зазначені системи якраз і призначені для їх недопущення або, в крайньому випадку, оперативного усунення. Для цього використовуються функції аналізу зібраної статистики та прогнозування, а також локалізації справжніх причин інцидентів.

Якщо підсумувати вище сказане, *моніторинг* – це комплекс швидкого реагування, надання і знаходження актуальної інформації для аналізу стану IT-інфраструктури, оповіщення про неї адміністраторів, а також діагностики, що дає повну і точну інформацію про виниклу несправність і її оперативне усунення.

Для вирішення проблеми моніторингу комп'ютерних мереж різної складності, як комерційних компаній, так і держструктур існує безліч програмних продуктів. В роботі ми розглянемо найбільш популярну систему розподіленого моніторингу корпоративного класу Zabbix.

Zabbix – це програмне забезпечення з відкритим вихідним кодом для моніторингу мереж і додатків. Він пропонує моніторинг в реальному часі зібраних з серверів, віртуальних машин, мережевих пристроїв і веб-додатків. Ці показники можуть допомогти вам визначити поточний стан вашої IT-інфраструктури і виявити проблеми з апаратними або програмними компонентами.

Будь-яка система моніторингу, в тому числі моніторингу мережевих пристроїв, – це складна інформаційна система, що включає в себе основні компоненти (рис. 2.1):

Рис. 2.1. Основні компоненти моніторингу

Метрики мережевих пристроїв (CPU, температура, доступність пристроїв, втрати пакетів, помилки на інтерфейсах, доступна смуга пропускання та інші) - критично важливі параметри, за значеннями яких необхідно вести спостереження;

Моніторинг – процес збору, агрегування та аналізу метрик для поліпшення розуміння характеристик і поведінки компонентів системи. У цей пункт входить також візуалізація зібраних даних по метриках в різні графіки, діаграми, гістограми.

Систему оповіщень – не менш важливий компонент, оскільки виконує дії на основі змін значень спостережуваних метрик. При досягненні критичного порога значення метрики може спробувати самостійно виправити проблему за підготовленим сценарієм або відправити сповіщення відповідальній особі засобами SMS, електронної пошти та інші.

Zabbix використовує гнучкий механізм сповіщень, що дозволяє користувачам конфігурувати повідомлення засновані на e-mail практично для будь-якої події та мають безліч налаштувань сповіщень:

відправку повідомлень можна налаштувати, використовуючи розкладу ескалацій, одержувачів, типів сповіщень;

оповіщення можна зробити інформативними і корисними при використанні змінних макросів, що дозволяє швидко реагувати на проблеми з серверами.

Zabbix пропонує відмінні функції звітності та візуалізації даних засновані на даних історії. Це робить Zabbix ідеальним для планування потужності.

Правильно налаштований, Zabbix може зіграти важливу роль у моніторингу IT інфраструктури. Це вірно і для маленьких організацій з декількома серверами і для великих організацій з безліччю серверів.

Zabbix – високо інтегроване рішення моніторингу мережі, яке пропонує безліч функцій в одному пакеті, варто відзначити основні особливості системи і виділити наступні [10]:

автоматичне виявлення серверів і мережевих пристроїв;

централізований моніторинг лог-файлів;

сервер може виконуватися під керуванням практично будь-який Unix-подібної операційної системи;

програма підтримує безліч платформ (Linux, Mac OS, Windows);

система моніторингу має готових агентів для більшості операційних систем Unix, Unix-подібних і Microsoft Windows;

система легко інтегрується з іншими системами завдяки прикладного інтерфейсу, реалізованому для безліч мов програмування;

моніторинг може здійснюватися за протоколами SNMP (v1, v2 і v3), IPMI, JMX, ODBC, SSH, HTTP (S), TCP / UDP і Telnet;

централізований веб-інтерфейс;

дана система моніторингу дозволяє нам створювати власні елементи та графіки і інтерполювати дані в режимі реального часу;

збір даних з використанням призначених для користувача інтервалів, що виконуються сервером / проксі і агентами;

час зберігання даних обмежена лише дисковим простором;

єдина точка збору інформації для користувачів;

безпечна авторизація користувачів;

можливість створювати карти мереж;

простота налаштування.

У Zabbix є чотири основні інструменти, за допомогою яких можна моніторити певну робочу середу і збирати про неї повний пакет даних для оптимізації роботи.

Zabbix-сервер – це ядро системи (центральний процес) програмного забезпечення Zabbix. Використовується для зберігання і обробки всієї інформації, а також сповіщає адміністраторів про виникаючі проблеми. Сервер виконує опитування і вилов даних, обчислює тригери, відправляє оповіщення користувачам. Він є центральним компонентом, яким Zabbix агенти і проксі повідомляють дані про доступність і цілісності систем. Сервер може самостійно віддалено перевіряти мережеві служби (такі як веб-сервера і поштові сервери), використовуючи прості перевірки сервісів. Сервер є головним сховищем, в якому

зберігаються всі конфігураційні, статистичні та оперативні дані, так само він розсилає повідомлення адміністраторам в разі виникнення проблем з будь-якої з спостережуваних систем.

Всі дані про конфігурацію Zabbix зберігаються в базі даних, з якою взаємодіє і сервер і веб-інтерфейс[24]. Наприклад, коли ви створюєте новий елемент даних використовуючи веб-інтерфейс (або API), запис про це додається в таблицю елементів даних в базі даних. Потім, раз в хвилину Zabbix сервер опитує таблицю елементів даних для отримання списку активних елементів даних, і зберігає цей список в кеш Zabbix сервера. Саме тому будь-які зміни в веб-інтерфейсі Zabbix будуть відображені в розділі останніх даних з затримкою до двох хвилин

Zabbix-проксі – цей процес, який збирає дані про продуктивність і доступність з декількох вузлів в локальне сховище. Після цього, він передає всю інформацію на сервер (єдиним пакетом), таким чином проксі працює від імені сервера. Всі зібрані дані локально буферизуються і потім відправляються Zabbix серверу, якому належить цей проксі.

Розгортання проксі не обов'язково, але може бути дуже корисно для розподілу навантаження одиночного Zabbix сервера. Якщо тільки проксі збирають дані, то обробка цих даних на сервері не так сильно навантажує CPU і I / O диска. Для Zabbix проксі потрібна окрема база даних. Zabbix проксі підтримує наступні бази даних SQLite, MySQL і PostgreSQL. Ви можете використовувати Oracle або IBM DB2 на свій власний ризик, при цьому можливі певні обмеження, наприклад в значеннях, що повертаються правилами низькорівневого виявлення.

Але це не єдина причина, по якій може знадобиться використання проксі. Він так само потрібен, якщо деякі агенти знаходяться в значно віддалених місцях, що позначається на величині пінга в їх доступності, або з якихось причин обмежені локальною мережею.

Zabbix проксі – ідеальне рішення для централізованого моніторингу віддалених об'єктів, філій та мереж, де відсутні локальні адміністратори.

Zabbix-агент – це програма (демон), яка встановлюється безпосередньо на спостережуване пристрій. Збирає всю інформацію (про локальні ресурсах і

додатках), яка після передається на сервер. Zabbix агенти розгортаються на спостережуваних цілях для активного моніторингу локальних ресурсів і додатків (статистика жорстких дисків, пам'яті, процесорів та інші).

Агент локально збирає оперативну інформацію і відправляє дані Zabbix сервера для подальшої обробки. У разі проблем (таких як відсутність вільного місця на жорсткому диску або аварійного завершення процесу сервісу), Zabbix сервер може швидко повідомити адміністраторів конкретного сервера, який повідомив про помилку. Zabbix агенти надзвичайно ефективні, тому що використовують рідні системні виклики для збору інформації статистики.

Zabbix-агенти підтримуються не тільки на nix операційних системах, а й на AIX та Windows.

Веб-інтерфейс – Zabbix пропонує потужний і одночасно простий у використанні веб-інтерфейс за допомогою якого здійснюється управління, та забезпечує доступ до інформації про стан вашої мережі і життєздатності ваших серверів з будь-якого місця. Реалізований на мові PHP, та для запуску вимагає наявність веб-сервера. Приклад на (рис. 2.2).

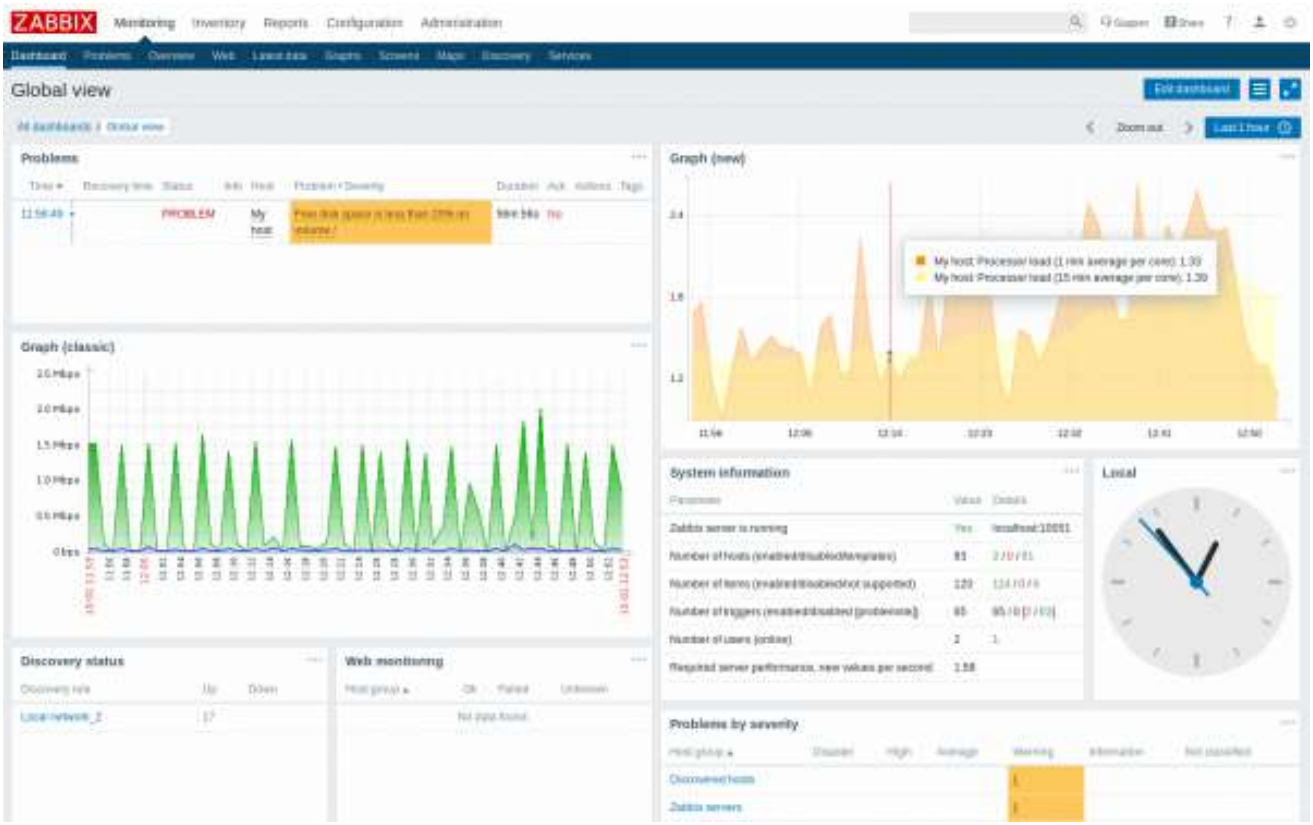

Рис. 2.2. Веб-інтерфейс системи моніторингу Zabbix

Веб-інтерфейс пропонує п'ять доступних функціональних розділів, включаючи:

Monitoring ("Моніторинг") - будь-яка інформація, яка налаштована в Zabbix на збір, візуалізацію і дії, буде відображатися в різних розділах Моніторингу;

Inventory ("Інвентарні дані") - інвентаризація включає розділи забезпечують огляд інвентарних даних вузлів мережі за обраним параметром, а також, можливість перегляду деталей інвентаризації вузлів мережі;

Reports ("Звіти") - включає в себе кілька розділів, які містять різні встановлені і призначені для користувача звіти, спрямовані на огляд таких параметрів як стан Zabbix, тригерів і зібраних даних;

Configuration ("Конфігурація") - містить розділи присвячені налаштування найважливіших функцій Zabbix, таких як вузли мережі і групи вузлів мережі, збір даних, пороги даних, відправка повідомлень про проблеми, створення візуалізації даних і багато іншого;

Administration ("Адміністрування") - використовується в Zabbix для адміністративних функцій. Це меню доступне тільки користувачам з типом "Super Admin".

Zabbix приваблює дуже зручним веб-інтерфейсом, в якому згруповані елементи керування і передбачає перегляд зібраних даних, їх налаштування.

Для безпеки входу здійснюється автоматичне від'єднання через 30 хвилин призначеного для користувача в стану бездіяльності, але після 5 невдалих спроб доступ блокується на 1 хвилину. А на головному екрані завжди відображається оновлена інформація про стан вузлів мережі і тригерів. Zabbix веб-інтерфейс передбачає управляти всією системою в одному інтерфейсі так і перегляд всіх зібраних даних.

Веб-інтерфейс забезпечеє більш легкого доступу до даних моніторингу і конфігурації системи Zabbix з будь-якого місця і з будь-якої платформи. Хоча одночасного використання двох інсталяцій веб-інтерфейсів Zabbix, на одному хості, але на різних портах, буде неуспішним.

Інтерфейс дозволяє відображення логічної структури мережі, яку можна вручну створювати карти мережі, що відображають саме розташування вузлів мережі і зв'язків між ними, причому поточний стан вузлів буде відображатися на карті за допомогою веб-інтерфейсу [9]. Приклад на (рис. 2.3).

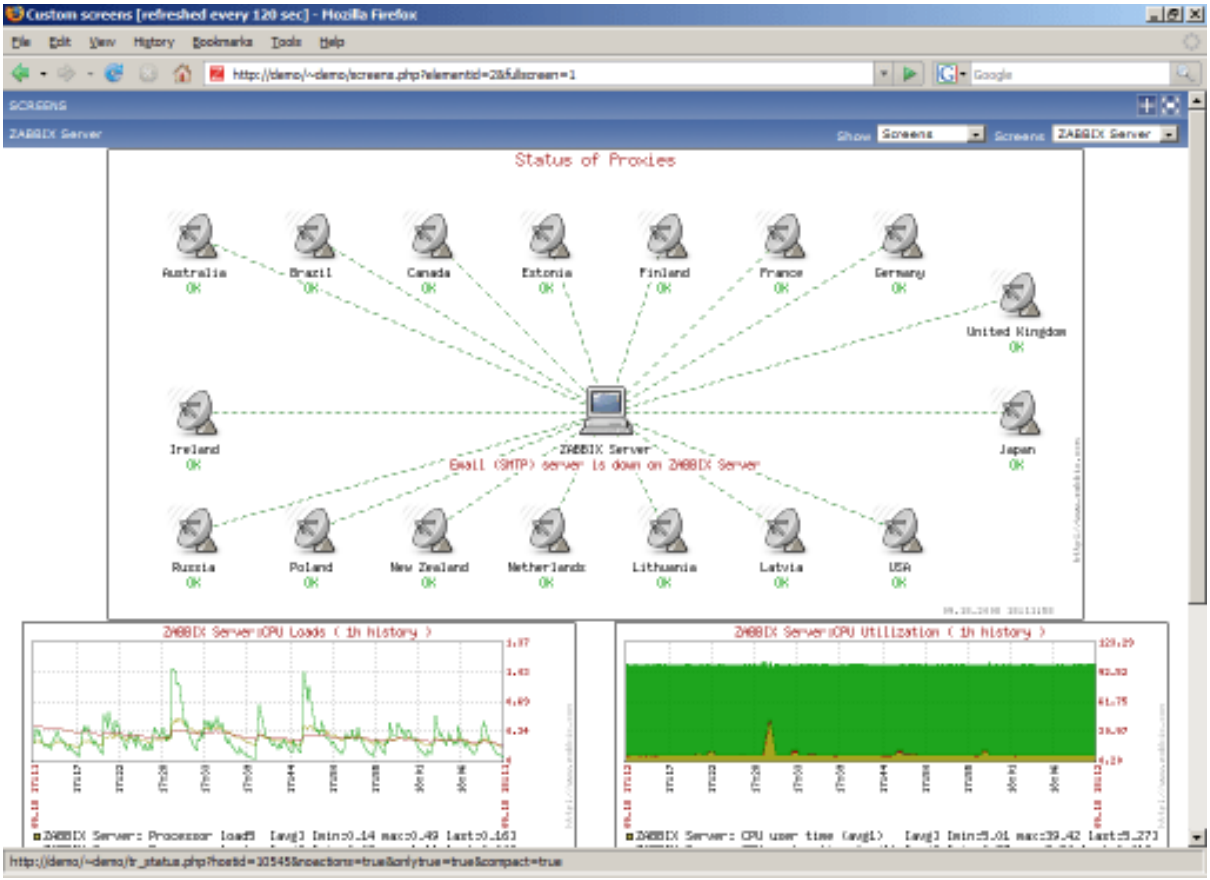

Рис. 2.3. Карти мережі системи моніторингу Zabbix

Веб-інтерфейс є частиною Zabbix сервера, і зазвичай (але не обов'язково), запущений на тому ж фізичному сервері що і Zabbix сервер. Також Zabbix використовує додаткові інструменти для моніторингу і збору даних:

Zabbix sender – це утиліта командного рядка, що посилає дані на Zabbix сервер для подальшої їх обробки.

Zabbix_get – утиліта для опитування агентів (використовується при налагодженні).

Архітектура Zabbix для великого оточення складається з трьох різних серверів / компонентів (які також повинні налаштовуватися з урахуванням високої доступності): веб-сервер, сервер баз даних, сервер Zabbix.

На (рис. 2.4) зображена трирівнева архітектура Zabbix.

Рис. 2.4. Трирівнева архітектура Zabbix

Повна інфраструктура Zabbix у великих середовищах дозволяє вводити додаткові компоненти, які грають дуже важливу роль. Це Zabbix-агенти і проксі-сервери Zabbix.

Приклад такої інфраструктури зазначений на (рис. 2.5).

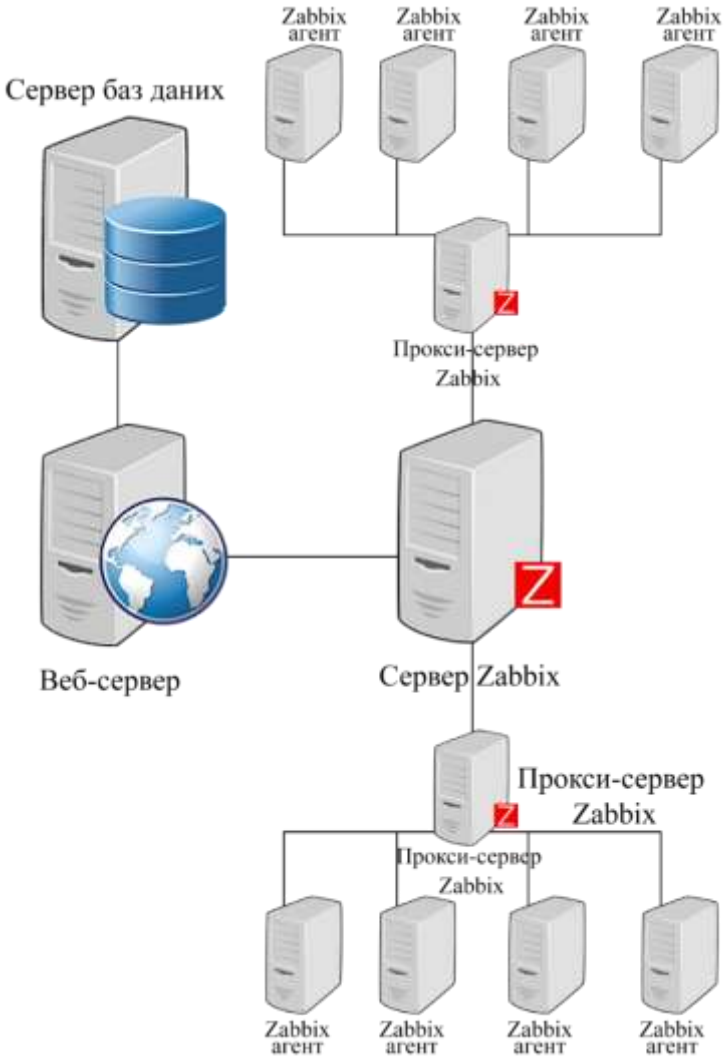

Рис. 2.5. Два додаткових компонента інфраструктури Zabbix

У цій інфраструктурі є централізований сервер Zabbix, до якого підключено кілька проксі-серверів, зазвичай по одному на ферму або підмережа.

Сервер Zabbix отримує дані від проксі-серверів Zabbix, проксі-сервери отримують дані від підключених до них агентів Zabbix, всі дані сохраняються в виділеної СУБД, а доступ до цих даних, звітів, та статистики Zabbix, так само як і параметри настройки, здійснюється за допомогою веб-інтерфейсу. Якщо заглянути в реалізацію системи, можна побачити, що веб-інтерфейс написаний на мові PHP, а сервер, проксі-сервери і агенти - на мові "C". Вибір мови "C" для реалізації сервера, проксі-серверів і агентів обумовлений прагненням забезпечити найвищу продуктивність і мінімальне споживання системних ресурсів. Всі компоненти оптимізовані на досягнення максимальної продуктивності.

Використовуючи проксі-сервери, можна реалізувати різні архітектури в порядку зростання складності: з єдиним сервером, з єдиним сервером і безліччю проксі-серверів та розподіленої архітектури.

Архітектура з єдиним сервером не передбачає використання у великому оточенні. Це найпростіша архітектура, де моніторинг здійснює єдиний сервер, яка може слугувати непоганою початковою точкою.

Моніторинг із застосуванням проксі-серверів реалізується шляхом настройки сервера Zabbix і декількох проксі-серверів, по одному на гілку або обчислювальний центр. Така конфігурація проста в обслуговуванні і має перевагу рішень централізованого моніторингу. Вона забезпечує хороший баланс між складністю реалізації та моніторингом великого оточення.

Zabbix – надзвичайно легким додатком моніторингу, якій здатний керувати тисячами елементів даних в конфігурації з єдиним сервером [26]. Однак, для моніторингу тисяч хостів в мережі зі складною топологією або розкиданих географічно-пов'язаними лініями з повільною або нестійким зв'язком конфігурації з єдиним сервером може виявитися недостатньо.

Крім того, необхідність переходу від монолітної конфігурації до розподіленої не завжди обумовлена недостатньою продуктивністю і тому не завжди зводиться до вибору між придбанням безлічі слабких комп'ютерів або

одного великого. На практиці часто зустрічаються мережі з сегментами, в яких діють суворі правила забезпечення безпеки, що не допускають двосторонні взаємодії між вузлами і відповідно не допускають можливості взаємодії сервера Zabbix з усіма агентами в таких сегментах. Різних підрозділах однієї компанії або різним компаніям в одній груп може знадобитися певна незалежність в управлінні їх мережами. Різні дослідницькі лабораторії можуть не мати надійного підключення до мережі. У таких випадках потрібно організувати накопичення контрольованих параметрів і їх передачу в асинхронному режимі для подальшої обробки.

Завдяки своїм можливостям розподіленого моніторингу Zabbix може з успіхом використовуватися у всіх перерахованих випадках і забезпечити працездатності здатне рішення незалежно від причин, будь то недостатня сегментація мережі, адміністративна незалежність або затримка даних через ненадійною зв'язку.

Ми також торкнемось питань забезпечення моніторингу безпеки за допомогою Zabbix, та взаємодії між сервером і проксі-серверами на рівні існуючих методів безпеки в системі Zabbix. Хоча спори про використання відкритого (opensource) в задачах забезпечення безпеки йдуть дуже давно. Як у прихильників, так у противників цієї ідеї накопичиться незаперечний запас аргументів на свій захист.

Однак, не дивлячись на це, в Zabbix є інструменти, які добре зарекомендували себе які підходять для цілей ІБ. Таким прикладом може послужити використання нових методів безпеки:

надійне шифрування між усіма компонентами Zabbix;

методи аутентифікації: Open LDAP, Active Directory;

гнучка схема прав доступу користувачів;

код Zabbix відкритий для аудиту безпеки.

Ще за допомогою Zabbix можна так само і дуже ефективно відстежувати події ІБ на мережевих пристроях Cisco і Juniper, використовуючи протокол SNMP. З точки зору ІБ можна виділити наступні події, які необхідно відстежувати - зміни

конфігурацій обладнання, виконання команд на комутаторі / маршрутизаторі, успішну авторизацію, невдалі спроби входу і багато іншого [11].

2.3 Аналіз існуючих методів двофакторної автентифікації користувачів інформаційних систем

В останній час передача даних по незахищених каналах зв'язку створює потенційну можливість для дій зловмисників. В інформаційних системах зберігається, обробляється, циркулює різна інформація, втрата або спотворення якої може завдати істотної шкоди. Тому для забезпечення інформаційної безпеки, одним із важливих завдань є використання методів і засобів безпечної автентифікації Для користувачів комп'ютерних технологій звичною є аутентифікація на основі логіна і пароля. Однак логін легко розпізнати, тому що в більшості випадків він збігається з адресою електронної пошти або номером телефону, а пароль можна зламати або відновити, наприклад, підбором відповіді на контрольні питання. У зв'язку з цим для більшої безпеки фахівці розробили багатофакторну автентифікацію. Поява цих технологій створило супутній попит на методи автентифікації, засновані не тільки на традиційних криптографічних методах (шифрування, хешування, цифровий підпис), але і на методах, заснованих використанні декількох факторів забезпечення достовірності особи, яка здійснює фінансову операцію. Основними пріоритетами в створюваних в наші дні методів багатофакторної автентифікації інформаційних систем є надійність (в контексті безпеки) і зручність її експлуатації, причому в першу чергу для кінцевого користувача.

Існування багатофакторної автентифікації (multi-factor authentication, MFA) полягає в тому, щоб взаємно компенсувати недоліки декількох окремих факторів, як мінімум двох, у яких розрізняються ключові ризики.

Методи багатофакторної автентифікації отримали в останнє десятиліття широке застосування в різних областях комунікаційних технолоігий, пов'язаних в першу чергу, з питаннями ідентифікації та допуску суб'єкта до конфіденційної

інформації. Хоча на практиці найчастіше використовується двофакторна автентифікація [13].

Двофакторна автентифікація two-factor authentication (2FA), також відома як двоетапна верифікація), є типом багатофакторної автентифікації. Двофакторна автентифікація є технологією, що забезпечує ідентифікацію користувачів за допомогою комбінації двох різних компонентів.

Двофакторна безпека вимагає одночасної присутності двох компонентів з боку користувача: "щось, що ви знаєте", і "щось, що ви маєте. Традиційні системи використовують ім'я користувача і пароль для автентифікації. Цей метод забезпечує міні-мінімальний рівень безпеки, оскільки імена і паролі можна легко перехопити і навіть іноді просто вгадати. Введення додаткового рівня безпеки забезпечує більш ефективний захист від несанкціонованого доступу. У разі двофакторной автентифікації пароль також використовується в ролі компонента "щось, що ви знаєте", тоді як в якості компонента "щось, що ви маєте" зазвичай виступає інструментом для отримання відповідного йому ключа доступу. Останнім може служити збережений на комп'ютері електронний сертифікат безпеки або прийшов на особистий телефон SMS з кодом підтвердження, або ж відбиток пальця, знятий зчитує електронним пристроєм.

Наприклад, систему, побудовану на апаратних ключах, які користувачі повинні мати при собі, можна підсилити за рахунок механізму паролів, які користувачі повинні пам'ятати. Тоді зловмисник з токеном не знатиме пароля, а зломщик, який вкрав пароль, не матиме токена. Звичайно, найпоширеніший і загальновідомий варіант двофакторної автентифікації - це два пароля, постійний і одноразовий; однак сутність цієї конструкції аналогічна описаній вище, тому що основний спосіб утримання доставки одноразового пароля залишається мобільний зв'язок. Іншими словами, справжнім визнається той користувач, який знає постійний пароль і має при собі смартфон, куди приходить пароль тимчасовий - так що пристрій зв'язку де-факто грає роль апаратного токена [14]. Інший фактор може включати те, що ви маєте, наприклад унікальний токен, щось що змінюється кожні

30 секунд (одноразовий пароль на основі часу) або щось таке, як, наприклад, відбиток пальця користувача.

Найпростіший приклад двофакторної автентифікації, з яким постійно стикається кожен з нас - це зняття готівки через банкомат. Щоб отримати гроші, потрібна карта, яка є тільки у вас, і PIN-код, який знаєте тільки ви. Отримавши вашу карту, зловмисник не зможе зняти готівку не знаючи PIN-коду і точно так само не може отримати гроші знаючи його, але не маючи карти. За таким же принципом двофакторної автентифікації здійснюється доступ до ваших акаунтів в соцмережах, до пошти та інших сервісів.

При розгляді різних методів двофакторної автентифікації, ми розглянемо їх переваги та недоліки. Виділимо основні часто використовувані ефективні методи систем двофакторної автентифікації.

Методи двофакторной автентифікації найчастіше використовуються у фінансовій сфері, але в принципі можуть застосовуватися практично в будь-який інший області.

Основні способи побудови систем двофакторної аутентифікації підрозділяються:

SMS.

Підтвердження за допомогою SMS-кодів працює дуже просто. Ви, як завжди, вводите свій логін і пароль, після чого на ваш номер телефону приходить SMS з кодом, який потрібно ввести для входу в обліковий запис. Це все. При наступному вході відправляється вже інший SMS-код, дійсний лише для поточної сесії. Це найпростіший спосіб. Користувачеві не потрібно ні додаток, ні смартфон. SMS з кодом може прийти на будь-яку модель мобільного телефону. Але цей спосіб вважається найменш надійним. SMS-повідомлення не зашифровані, тому хакери можуть отримати до них доступ.

Переваги:

генерація нових кодів при кожному вході, якщо зловмисники перехоплять ваш логін і пароль, вони нічого не зможуть зробити без коду;

SMS приходить на телефон, кожен може скористатися цією опцією - незалежно від наявності інтернету;

прив'язка тільки до вашого телефонного номеру, без вашого телефону вхід неможливий.

Недоліки:

при відсутності сигналу мережі ви не зможете ввести логін та пароль;

підміна номера через послугу оператора або працівників салонів зв'язку;

мобільний телефон повинен ловити мережу, коли відбувається автентифікація, інакше SMS повідомлення з паролем не дійде;

текстові повідомлення (SMS), які, потрапляючи на ваш мобільний телефон, можуть бути перехоплені.

сучасні смартфони використовуються, як для одержання пошти, так і для отримання SMS. Як правило електронна пошта на мобільному телефоні завжди включена. Таким чином, усі акаунти, для яких пошта є ключем, можуть бути зламані (перший фактор). Мобільний пристрій (другий фактор).

Гіпотетично метод автентифікації у вигляді SMS можна назвати зручним способом (багато хто вірять у високу безпеку SMS-кодів), тим не менше, автоматична розсилка іноді дає збої примушуючи чекати користувача деякий час. Судячи з принципу роботи цього методу автентифікації можна припустити, що він є безпечним, однак навіть те, що ваш телефонний номер належить лише вам, цього недостатньо для забезпечення абсолютної захищеності цього способу.

U2F Ключі.

Універсальний 2-й фактор (Universal 2nd Factor – U2F) - це пристрій який є другим фактором в протоколах або реалізаціях систем двофакторної аутентифікації за участю людини. Наприклад, на додаток до паролю, інформаційна система також перевірить що користувач має даними екземпляром U2F пристрою. Принцип дії заснований на зберіганні в аутентифікації типу «питання-відповідь» (challenge response) за допомогою цифрового підпису, і обов'язкової участі людини. U2F - це відкритий стандарт, який використовується з пристроями USB, NFS та смарт-картками. Щоб автентифікуватися, ви маєте просто підключити його (для USB -

ключів), натиснути на нього (для пристроїв NFS або провести смарт-картою) до обладнання.

Переваги:

ключ U2F - справжній фізичний фактор. На відміну від SMS -кодів, їх не можна перехопити або перенаправляти. І на відміну від більшості двофакторних методів, ключі U2F є захищеними від фішингу, оскільки вони зареєстровані лише для роботи з конкретними сайтами, на яких ви зареєстровані. Це один з найнадійніших методів 2FA в даний час.

Недоліки:

U2F - відносно нова технологія, вона ще не так широко підтримується. Наприклад, ключі NFS працюють лише з мобільними пристроями Android, тоді як USB-ключі працюють переважно з браузером Chrome;

ключі U2F також коштують грошей, часто від 10 до 60 доларів, але можуть збільшитися в залежності від того, наскільки міцний ключ ви хочете.

U2F - це добре продумана, відкрита і стандартизована технологія, яка була успішно протестована Google на своїх співробітниках, котрі використовують U2F на даний момент в якості основного методу двофакторної аутентифікації.

Додатки-автентифікатори.

Цей варіант багато в чому схожий на SMS, з тією відмінністю замість отримання кодів по SMS, вони генеруються на пристрої за допомогою спеціального додатку (Google Authenticator, Authy). Ця програма виконує роль умовного центру розсилки SMS-повідомлень з кодами, тільки знаходиться завжди під рукою і не вимагає підключення до мережі. Google Authenticator можна налаштувати не тільки для корпоративних акаунтів, але і будь-якому приватному користувачеві. Під час налаштування ви отримуєте первинний ключ (у вигляді QR-коду), на основі якого за допомогою криптографічних алгоритмів генеруються одноразові паролі з терміном дії від 30 до 60 секунд. Користувачі Google можуть використовувати звичну схему з прив'язкою логіна і пароля до номера телефону, використовуючи Google Authenticator або придбати електронний ключ для більш безпечної аутентифікації.

Переваги:

не потрібен сигнал мережі для автентифікатора, тобто достатньо підключення до інтернету лише при первинному налаштуванні;

підтримка декількох акаунтів в одному автентифікаторі.

Недоліки:

якщо зловмисники отримають доступ до первинного ключа на вашому пристрої або шляхом злому сервера, вони зможуть генерувати паролі в майбутньому.

При використанні автентифікатора на тому ж пристрої, з якого здійснюється вхід, втрачається двофакторність.

Перевірка входу за допомогою мобільних додатків.

Даний тип автентифікації можна назвати збірною солянкою з усіх попередніх. В цьому випадку, замість запиту кодів або одноразових паролів, ви повинні підтвердити вхід з вашого мобільного пристрою з встановленим додатком сервісу. На пристрої зберігається приватний ключ, який перевіряється при кожному вході. Це працює в Twitter, Snapchat-і та різних онлайн-іграх. Наприклад, при вході в ваш Twitter-аккаунт в веб-версії ви вводите логін і пароль, потім на смартфон приходить повідомлення із запитом про вхід, після підтвердження якого в браузері відкривається ваша стрічка.

Переваги:

не потрібно нічого вводити при вході;

незалежність від мережі;

підтримка декількох акаунтів в одному додатку;

Недоліки:

якщо зловмисники перехоплять приватний ключ, вони зможуть видавати себе за вас;

сенс двофакторної автентифікації втрачається при використанні одного і того ж пристрою для входу.

Апаратні токени.

Фізичні (або апаратні) токени є самим надійним способом двофакторної автентифікації. Будучи окремими пристроями, апаратні токени, на відміну від всіх

перерахованих вище способів, ні при якому розкладі не втратять своєї двофакторної складової. Найчастіше вони представлені у вигляді USB-брелоків з власним процесором, що генерує криптографічні ключі, які автоматично вводяться при підключенні до комп'ютера. Вибір ключа залежить від конкретного сервісу. Google, наприклад, рекомендує використовувати маркери стандарту FIDO U2F, ціни на які починаються від 6 доларів без урахування доставки.

Переваги:

ніяких SMS і додатків;

немає необхідності в мобільному пристрої:

є повністю незалежним девайсом.

Недоліки:

потрібно купувати окремо;

підтримується не у всіх сервісах;

при використанні декількох акаунтів доведеться носити цілу в'язку токенов.

Резервні ключі.

По суті, це не окремий спосіб, а запасний варіант на випадок втрати або крадіжки смартфону, на який мають приходити одноразові паролі або коди підтвердження. При налаштуванні двофакторної автентифікації в кожному сервісі вам дають кілька резервних ключів для використання в екстрених ситуаціях. З їх допомогою можна увійти в ваш акаунт, відв'язати налаштовані пристрої та додати нові. Ці ключі варто зберігати в надійному місці, а не у вигляді скріншоту на смартфоні або текстового файлу на комп'ютері.

Біометрія.

Біометрична система аутентифікації дуже зручна для користувачів, яка розпізнає людей на основі їх анатомічних особливостей або поведінкових рис [29]. На відміну від систем, що використовують паролі, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи автентифікації засновані на людських параметрах, які завжди знаходяться разом з ними. Розпізнавання обличчя, розпізнавання голосу та сканування відбитків пальців підпадають під категорію біометричних даних. Системи використовують біометричну автентифікацію, коли

потрібно, щоб ви дійсно були тими, за кого себе видаєте, часто в областях, де потрібна перевірка безпеки (наприклад, уряд, фінансові установи) [29].

У всіх біометричних технологій існують загальні підходи до вирішення завдання ідентифікації, хоча всі методи відрізняються зручністю застосування, та точністю результатів. Будь-яка біометрична технологія застосовується поетапно:

сканування об'єкта;

витяг індивідуальної інформації;

формування шаблону;

порівняння поточного шаблону з базою даних.

Біометрична аутентифікація грунтується на унікальності ряду характеристик людини. В даний час методи біометричної аутентифікації діляться на два класи:

1. Статичні методи, засновані на фізіологічних характеристиках людини, що знаходяться при ньому протягом всього його життя, і які не можна втратити, вкрасти або скопіювати.

До статичних методів автентифікації належать:

код ДНК;

сітківка ока;

райдужна оболонка ока;

термограма обличчя (теплове зображення обличчя);

відбитки пальця, (папілярна лінія пальців);

геометрія руки (геометрія кисті руки);

2. Динамічні методи, засновані на поведінкових характеристиках людей.

Динамічними методами автентифікації є:

голос;

рукописний почерк;

клавіатурний почерк;

В процесі біометричної аутентифікації пред'явлений користувачем зразки порівнюють з деякою погрішністю, яка визначається і встановлюється заздалегідь. Похибка підбирається для встановлення оптимального співвідношення двох основних характеристик біометричної аутентифікації:

FAR (False Accept Rate) - коефіцієнт помилкового прийняття (тобто такий собі успішно пройшов аутентифікацію під ім'ям легального користувача).

FRR (False Reject Rate) - коефіцієнт помилкового відмови (тобто легальний користувач системи не пройшов аутентифікацію).

FAR і FRR вимірюються у відсотках і повинні бути мінімальні. Дані величини є зворотньозалежну, тому в залежності від використовуваної біометричної характеристики і вимог до якості захисту шукається якась «золота середина» між даними величинами. Серйозне засіб біометричної аутентифікації повинно дозволяти налаштувати коефіцієнт FAR до величин порядку 0,01-0,001% при коефіцієнті FRR до 3-5%.

Переваги:

Біометрію надзвичайно важко підробити. Навіть відбиток пальців, який, можливо, найпростіший для копіювання, вимагає певного фізичної взаємодії.

Розпізнавання голосу потребує певного твердження сказаного вашим голосом.

Розпізнавання обличчя потребує чогось радикального, такого як пластична хірургія. Він не незламний, але досить близький до цього.

Недоліки:

загроза безпеки на все життя;

ймовірність зміни зловмисником бази шаблонів;

біометричні дані людини змінюються (в результаті старіння, травм, опіків, порізів, хвороби, ампутації, тощо), тому база шаблонів потребує постійного оновлення;

крадіжка біометричних даних або їх компрометація;

біометричні характеристики є унікальними, але їх не можна зберегти в секреті;

більшість біометричних систем є дорогими для широкого використання;

Найбільший недолік і причина, чому біометрія рідко використовується як двофакторний метод, полягає в тому, що скомпрометований біометричний пристрій може ставити під загрозу саме життя.

Важливий недолік біометричної аутентифікації - необхідність в сканерах для зчитування біометричних характеристик користувача, які є досить дорогими на ринку.

Потрібно відзначити, що біометричні дані частіше використовують для ідентифікації, автентифікацію вже проводять за допомогою призначених для користувача паролів.

Отже, якщо використовувати вищевказані методи двофакторної автентифікації, то може значно підвищити рівень безпеки вашого акаунту. Хоча є багато сервісів, які мають SMS верифікацію, надсилаючи коди через текстові повідомлення на ваш телефон, коли ви намагаєтеся ввійти. Використовуючи автентифікацію в якості SMS-повідомлення мають багато проблем із безпекою та являються найменш захищеним методом для двофакторної автентифікації [14].

Обов'язково використовуйте на своїх пристроях (смартфон, ноутбук, ПК та інші) багатофакторну аутентифікацію, як основний рівень захисту при вході в обліковий запис, та на будь-які сайти, що зберігають ваші особисті дані (соцмережі, електронна пошта та інші), навіть якщо сервіс дозволяє обійтися без неї. Звичайно, це не завжди зручно, але практично завжди робить відвідування важливих сайтів більш безпечним. При цьому для критично важливих даних використання USB-токенів або біометричної автентифікації - більш кращий варіант, ніж одноразові SMS-паролі. Саме тому Національний інститут стандартів і технологій більше не рекомендує використовувати SMS-повідомлення для двофакторної автентифікації.

Таким чином, найкращим прикладом двофакторної автентифікації є авторизація Google і Microsoft. Коли користувач заходить з нового пристрою, крім автентифікації по імені та паролю, його просять ввести шестизначний (Google) або вісьмизначний (Microsoft) код підтвердження [13]. Отримати його можна за допомогою SMS, або голосового дзвінка на телефон, він може бути взятий з заздалегідь складеного реєстру разових кодів або можна використовувати додаток-автентифікатора, генеруючий новий одноразовий пароль за короткі проміжки часу.

3 РОЗРОБЛЕННЯ РЕОМЕНДАЦІЙ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ СИСТЕМИ ZABBIX ІЗ ЗАСТОСУВАННЯМ ДВОФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

3.1 Технологія забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix

Як відомо, однією з найважливіших частин IT інфраструктури сучасних підприємств та приватних компаній є безліч найрізноманітніших систем, що генерують великий потік даних, та подій інформаційної безпеки, переглянути які всі просто неможливо. В таких умовах гостро стоїть проблема підтримки роботи розподіленої мережі на заданому рівні що є складною задачею і вирішувати ці завдання допомагають системи централізованого моніторингу та управління мережею передачі даних.

Існує безліч готових систем, як вільно розповсюджених, так і комерційних, але перш ніж впроваджувати будь-яку з них у виробничий процес, необхідно провести ретельний аналіз і врахувати всі ризики, пов'язані із застосуванням таких систем на окремо взятій інфраструктурі.

Найчастіше подібні системи мають вразливість в програмному забезпеченні і здійснюють передачу даних у відкритому вигляді, а зловмисник має можливість перехопити та фальсифікувати дані моніторингу, що серйозно обмежує сферу застосування деяких систем, особливо у великих компаніях. Для того, щоб впровадити систему в діючу інфраструктуру, необхідно врахувати декілька параметрів. Система повинна включати в себе інструменти захисту від несанкціонованого доступу збоку зловмисників (хакерів), безпечну передачу даних, модулі, які дозволяють здійснювати управління мережевим обладнанням, робочими станціями і серверами, як в ручному режимі, так і автономному. Перш за все, система розподіленого моніторингу повинна відповідати декільком вимогам:

висока безпека;

висока швидкість впровадження;

мінімальна кількість матеріальних витрат на впровадження;

підтримка сучасних мережевих протоколів і технологій;

взаємодія з наявними програмними продуктами.

Критерії вибору системи розподіленого моніторингу вимогливі і ним відповідає одна з таких систем - Zabbix. Значна увага при створенні вказаної системи приділяється забезпеченню безпеки цілісності і конфіденційності даних.

Zabbix - це розподілена система моніторингу (open-source) корпоративного рівня. На поточний момент одна з найпопулярніших і функціональних безкоштовних систем моніторингу. Основна задача системи полягає в зборі необхідної інформації, ретельному аналізі та регулярному проведені моніторингу, яке забезпечує своєчасне виявлення помилок і, відповідно, їх виправлення в найкоротші терміни. Окрім розподіленого моніторингу корпоративної мережі, основним завданням постає захист та забезпечення системи, спрямований на підвищення захищеності від несанкціонованого доступу.

Zabbix відповідає всім вимогам захисту та надійністю при передачі даних всередині корпоративної мережі, в якій відбувається моніторинг подій та сбір інформації з пристроїв, але може виникнути ситуації, при яких стан системи стає вразливий. Тобто, загроза інформаційної безпеки може проявитись не самостійно, а через можливу взаємодію, тобто через фактори вразливості. Якщо розглянути стан захищеності системи Zabbix, при детальному вивченні можна побачити слабкі та вразливі ланки в програмно-техничному забезпеченні та адмініструванні.

Програмне забезпечення Zabbix дуже різноманітне і вміщує багато потужних і гнучких інструментів, тим самим викликає особливий інтерес зі сторони зловмисників, які можуть спробувати скористатися наявними можливостями системи в своїх цілях. Завдяки можливостям Zabbix, маючи доступ до системи моніторингу, безпеки і конфігурації, хакери можуть здійснити атаки на хости, моніторинг яких здійснюється за допомогою Zabbix. При певних налаштуваннях зловмисник може перехопити (zbx_sessionid) далі створити нового користувача з правами адміністратора і закріпитись в системі Zabbix. Використовуючи

особливості роботи Zabbix-агента, зловмисник (при певних налаштуваннях агента) може проникнути на всі ПК, які моніторяться Zabbix-сервером.

Щоб запобігти несанкціонованого доступу хакерів до системи Zabbix і дій спрямованих на отримання незаконної вигоди та заподіяння шкоди інформації, які можуть призвести до порушення діяльності системи. Необхідно провести превентивні заходи с забезпеченням захисту системи, використовуючи:

існуючи методи та інструменти захисту системи Zabbix (автентифікація шифрування, розмежування прав доступу користувачів та інші);

плагін Zabbix Threat Control як сканер ІБ;

протокол SNMP в Zabbix для відстежування події ІБ на мережевих пристроях Cisco і Juniper за допомогою трапів (SNMP Trap).

1. Існуючи методи та інструменти захисту системи Zabbix.

Значна увага при створенні системи моніторингу приділяється забезпеченню безпеки даних. При цьому система підтримує шифрування як на рівні збережених даних, так і в рамках протоколів взаємодії між своїми компонентами не впливаючи на продуктивність системи. Налаштовані алгоритми шифрування і можливість визначення чорних і білих списків для метрик, дуже важливі для тих, кому вкрай важлива збережена інформація.

В налаштуванні зашифрованими сполуками Zabbix використовує на вибір:

RSA шифрування на основі сертифікатів;

PSK шифрування на основі ключів .

Використовуючи шифрування на основі алгоритмів RSA та PSK ключів, користувач (адміністратор) системи Zabbix отримував надійний безпечний та захист між компонентами:

Zabbix сервер;

Zabbix проксі;

Zabbix агент;

Zabbix_sender;

Zabbix_get.

Що значно підвищує рівень безпеки передачі даних в корпоративної мережі.

З виходом нової версії Zabbix 5.0 система моніторингу стала використовувіти захищене з'єднання із базою даних і це дає можливість налаштовувати безпечні з'єднання за допомогою протокола TLS 1.2 з базами даних MySQL і PostgreSQL з зовнішнього інтерфейсу або сервера Zabbix. Раніше цей функціонал був відсутній, що виникало безліч питань безпечної передачі даних між MySQL і PostgreSQL.

Для підтримки шифрування Zabbix, система повинна бути скомпільована і пов'язана з однією з чотирьох криптографічних бібліотек [10]:

OpenSSL;

LibreSSL;

GnuTLS;

Mbed TLS.

Все це дає можливість використовувати Zabbix в тих системах, де шифрування між вузлами є обов'язковою умовою.

Для безпечного та захищеного входу в систему, Zabbix пропонує розширені опції безпечної автентифікації та гнучку схему доступу користувачів, які доступні із застосуванням веб-інтерфейсу.

Основні методи автентифікації, які використовує Zabbix це:

Open LDAP;

Active Directory.

При налаштуванні автентифікації, адміністратор на вибір обирає більш зручний та надійний спосіб для входу в систему.

В Zabbix є можливість задати глобальний метод автентифікації, використовуючи веб-інтерфейс Zabbix. На вибір є кілька способів автентифікації:

автентифікація через внутрішню базу даних;

HTTP автентифікація;

LDAP автентифікація.

Глобальна підтримка шифрування та взаємної автентифікації в Zabbix дає можливість користувачам поступово і вибірково покращувати безпеку компонентів системи моніторингу і тим самим підвищувати рівень захищеності на високому рівні. Також можна зазначити надійну підтримку криптографії для паролів: більш

надійна криптографія bcrypt тепер використовується для хеширования призначених для користувача паролів замість MD5.

Управління доступом в системі дозволяє налаштовувати ієрархічні права доступу для користувачів і їх груп аж до конкретних об'єктів моніторингу, роблячи можливим створення політик доступу для організацій з територіально розподіленою філіальною структурою.

2. Zabbix Threat Control.

Для забезпечення додаткового захисту системи моніторингу в корпоративній мережі розподіленої інфраструктури, можна використовувати більш гнучкі та легкі інструменти, які будуть ефективно відстежувати події інформаційної безпеки.

Цим вимогам відповідає Zabbix Threat Control - плагін з відкритим вихідним кодом, написаний на Python, який дозволяє перетворити систему моніторингу Zabbix в сканер безпеки та систему управління вразливими, ризиками і безпекою для вашої інфраструктури за участю системи Vulners.

Vulners - це дуже велика і безперервно обновлювана база даних ІБ-контента, що дозволяє шукати вразливості, експлоїти, патчі, результати bug bounty, плагіни для OpenVAS, NESSUS, Burp Suite, правила для IPS / IDS та багато іншого. Vulners агрегатор даних про уразливість з більш ніж 115 джерел.

Zabbix Threat Control надає Zabbix розширену інформацію про вразливість, що існують у всій вашій інфраструктурі, і пропонує застосовні плани виправлення.

Основні функціональні можливості Zabbix Threat Control:

використовуючи Zabbix API, плагін отримує списки встановлених пакетів, імен і версій ОС з усіх серверів в інфраструктурі (якщо з ними пов'язаний шаблон «Vulners OS-Report»), а потім віддає це все ZTC;

передає дані в Vulners зіставляє всі дані з базою вразливостей і багів та повертає результат в Zabbix Threat Control;

обробляє отриману інформацію, агрегує її і відправляє назад в Zabbix через плагін zabbix-sender;

відображає в веб-інтерфейсі Zabbix інформацію про уразливість, знайдених у вашій інфраструктурі в Zabbix;

пропонує легко застосовні способи усунення знайдених вразливостей;

дозволяє корелювати дані з різних джерел;

отримує інформацію про уразливість для кожного сервера;

показує рівень загрози кожної вразливості за стандартом CVSS;

Загальна система оцінки вразливостей (CVSS) – це відкрита схема, яка дозволяє обмінюватися інформацією про IT-вразливості. Система оцінки CVSS складається з 3 метрик: базова метрика, тимчасова метрика і контекстна метрика. Кожна метрика являє собою число (оцінку) в інтервалі від 0 до 10 і вектор - короткий текстовий опис зі значеннями, які використовуються для виведення оцінки. Базова метрика відображає основні характеристики уразливості. Тимчасова метрика відповідає таким характеристикам уразливості, які змінюються з часом, а контекстна метрика – характеристикам, які є унікальними для середовища користувача.

Для повноцінного функціонування плагіну, система Zabbix повинна бути розгорнута на основі ОС Linux і включати в себе додаткові компоненти.

Установка проходить в кілька етапів:

установка Zabbix-сервера

установка Zabbix-агент на хости які відслідковуються;

установка ZTC на хости які відслідковуються;

установка ZTC на сервер.

Також необхідно встановити додаткові плагіни :

zabbix-sender потрібен для відправки в даних про уразливість в систему моніторингу;

zabbix-get для відправки fix-команд, які виправляють уразливості, на серверах.

python v3 з модулями: pyzabbix, jpath, requests для запуску основних скриптів плагіна.

zabbix-agent для збору даних і запуску скриптів.

Після створення в Zabbix всіх об'єктів скрипт покаже:

посилання на створений дашборда в Zabbix, на якому будуть відображатися уразливості;

час, коли буде запускатися сканування інфраструктури на уразливості.

Після виконаної роботи відкриваємо новий дашборд ZTC (рис. 3.8), переходимо в шаблони і обираємо Vulners OS-Report. У розділі "Hosts" необхідно вказати, перемістивши їх в лівий textbox, ті сервери, які вимагають сканування. Чекаємо, поки програма сканує хости, і отримуємо результати. Після цього залишається дочекатися запуску плагіна в вказане при інсталяції час.

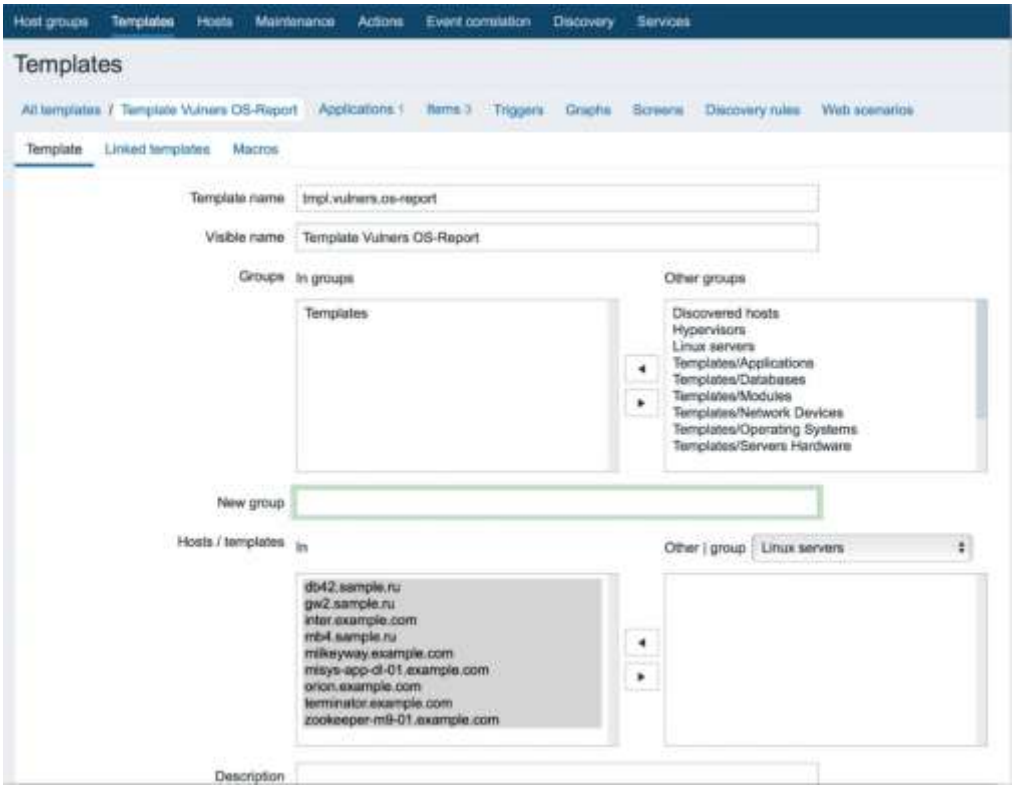

Рис. 3.1. Дашборд ZTC в веб-інтерфейсі Zabbix

Запуск основного скрипта обробки даних (ztc.py) відбувається автоматично, один раз на добу, через "Service Item ..." на хості "Vulners - Statistics" в вказане скриптом час.

Можна поміняти час запуску плагіна на будь-який зручний, змінивши "Scheduling interval" в цьому елементі даних. При цьому необхідно відкоригувати час збору статистики в трьох елементах даних шаблону "Vulners OS-Report" - метрики в шаблоні повинні спрацьовувати хвилин на 10 ... 15 раніше, ніж основна метрика "Service Item ..." на хості "Vulners - Statistics" [12].

Час, за яке буде опрацьовано всі дані про вразливість залежить від кількості серверів в інфраструктурі і кількості встановлених на них пакетів. Орієнтовно на обробку 1 тисячі серверів витрачається близько 30 хвилин.

Після закінчення сканування отримуємо приблизно такий висновок результатів:

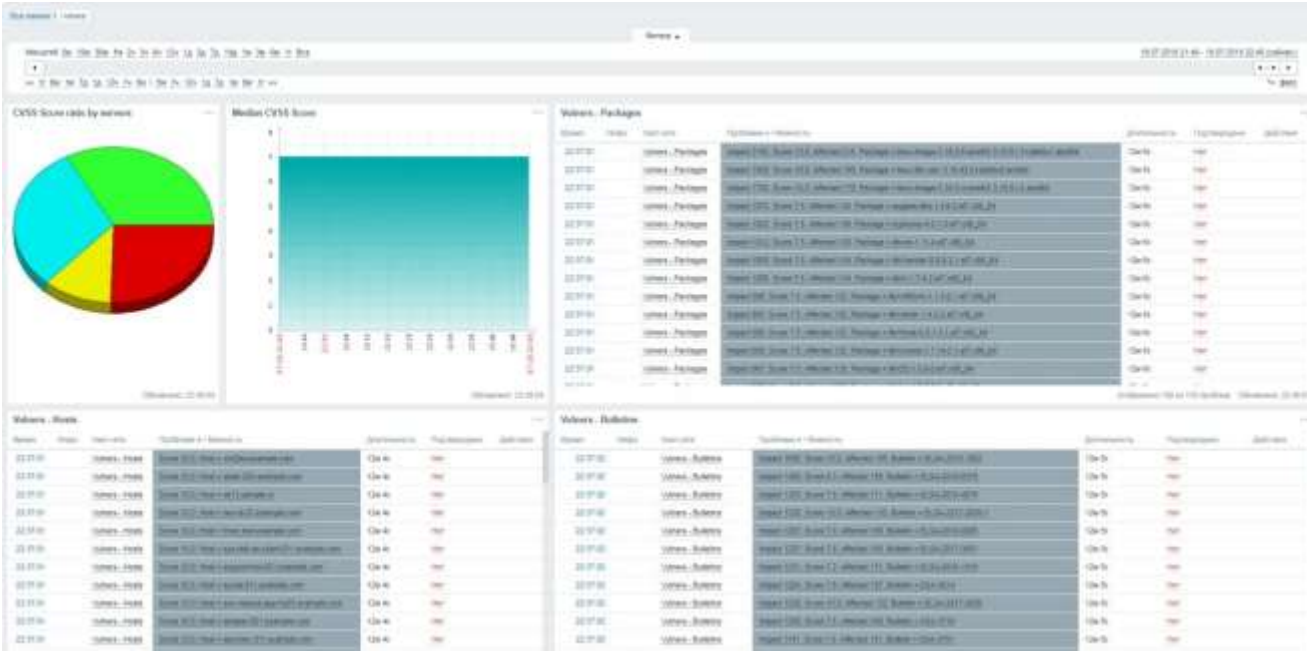

Рис. 3.2. Діаграма результатів сканування на дашборді ZTC

На діаграмі (рис. 3.2) червоним виділені критичні уразливості, що мають дуже високий бал за CVSS. Всі дані зручно відсортовані в декількох панелях: по вразливих пакетам, вразливостей по серверам. Відповідно, виправити можна або все уразливості на конкретно обраному сервері, або певну вразливість на всіх серверах.

Загальна інформація буде відображатися в веб-інтерфейсі Zabbix в наступному форматі:

максимальна оцінка CVSS для кожного сервера;

команда для виправлення всіх виявлених вразливостей для кожного сервера;

список бюлетенів безпеки з описами вразливих пакетів, дійсних для вашої інфраструктури;

список всіх вразливих пакетів у вашій інфраструктурі.

Інформація про бюлетені безпеки і пакетах включає в себе:

індекс впливу на інфраструктуру;

CVSS оцінка пакета або бюлетеня;

кількість порушених серверів;

докладний список порушених хостів;

гіперпосилання на опис бюлетеня.

Іноді неможливо оновити всі пакети на всіх серверах до версії, яка усуває існуючі уразливості. Пропоноване уявлення дозволяє вам вибірково оновлювати сервери або пакети. Такий підхід дозволяє виправляти вразливості, використовуючи різні стратегії: всі уразливості на конкретному сервері та єдина вразливість у всій інфраструктурі. Це можна зробити безпосередньо з Zabbix (використовуючи його стандартні функції) або по команді адміністратора, або автоматично.

Інформацію вразливостей на серверах, як і про командах для усунення проблем, можна отримати в підказках, (рис. 3.3) які активуються при наведенні на проблему. Там же будуть представлені посилання на vulners.com, де можна ознайомитися з проблемами ІБ, що стосуються даних серверів.

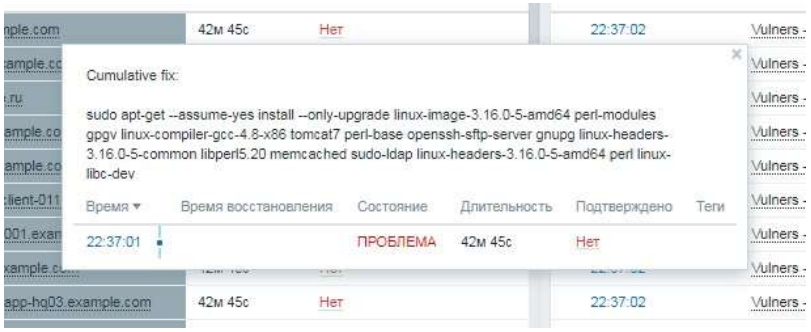

Рис. 3.3. Усунення проблем через підсказки

Для установки оновлень необхідно підтвердити проблему. Особливо зручно це буде для тих, хто хоче усунути одну з вразливостей на всіх серверах, якщо немає систем управління типу Ansible.

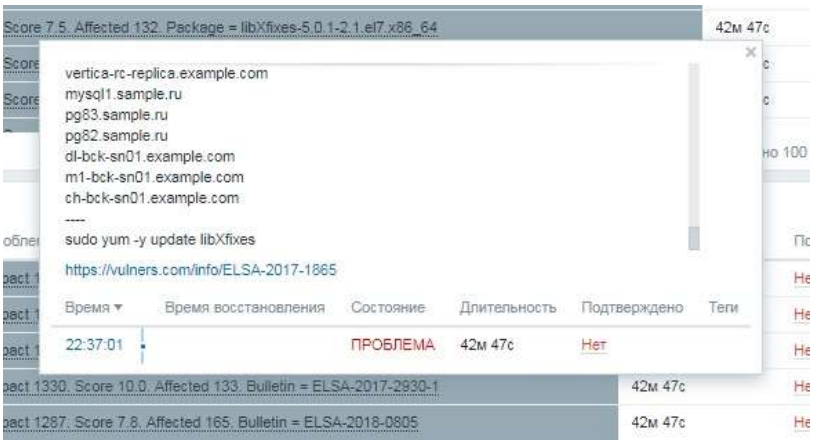

Рис. 3.4. Установки оновлень через підтвердження проблеми

У підсумку, після інсталяції необхідних пакетів і збору інформації Zabbix Threat Control покаже всі сервери в мережі, які схильні до тих чи інших вразливостей через невстановлених патчів або старих версій пакетів. Інформація про уразливість виводиться у вигляді проблем, які можна або ігнорувати (просто закривши її, не підтверджуючи), і ніякої дії не буде, або підтвердити, після чого агентам відправиться fix-команда, яка усуне вразливість.

Запропонований в плагіні підхід дозволяє вибирати підходящу вам стратегію усунення вразливостей:

Одна вразливість у всій інфраструктурі: якщо для вас критична якась певна вразливість - плагін надає вам інформацію де у вашій інфраструктурі ця вразливість існує, і яким чином її можна виправити відразу у всій інфраструктурі.

Всі уразливості на певному сервері: якщо вам необхідно мати цілком безпечний сервер, наприклад знаходиться в DMZ або за периметром компанії - використовуючи плагін ви отримуєте інформацію про те як усунути всі знайдені на ньому уразливості.

На даний момент Zabbix Threat Control вимагає Zabbix версії не нижче 3.4 та здатний працювати тільки з ОС Linux, але, можливо, будуть розроблені пакети під інші ОС (в тому числі активне мережеве обладнання).

3. Моніторинг подій ІБ на мережевих пристроях.

За допомогою Zabbix можна так само дуже ефективно відстежувати події ІБ на мережевих пристроях Cisco и Juniper, використовуючи протокол SNMP.

Передача даних з пристроїв здійснюється за допомогою так званні трапів (SNMP Trap) [9].

З точки зору ІБ можна виділити наступні події, Які необхідно відстежувати – Зміни конфігурацій обладнання, виконання команд на комутаторі / маршрутизаторі, успішну авторизацію, невдалі спроба входу і багато іншого.

Основні способи моніторингу ІБ на мережевих пристроях:

Розглянемо приклад з авторизацією, на тестову стенді використовуватиме емулятор GNS3 з маршрутизатором Cisco 3745.

Для початку нам необхідно налаштувати відправку SNMP трапів з маршрутизатора на сервер моніторингу:

login block-for 30 attempts 3 within 60

login on-failure log

login on-success log

login delay 5

logging history 5

snmp-server enable traps syslog

snmp-server enable traps snmp authentication

snmp-server host 192.168.1.1 public

Будемо відправляти події з Syslog і трапи аутентифікації. Зауважу, що вдалі і невдалі спроби авторизації пишуться саме в Syslog. Далі необхідно налаштувати прийом потрібних нам SNMP трапів на сервері моніторингу.

У нашому прикладі будемо ловити трапи Syslog. Тепер необхідно налаштувати елемент даних для збору статистики з наступним ключем:

snmptrap[“Status”]

Якщо трап не налаштований на сервері моніторингу, то в лог-файлах сервера будуть приблизно такі записи:

unmatched trap received from [192.168.1.14]: ...

В результаті отриманих лог-файлів (рис. 3.5) буде відображатися інформація про спроби входу з деталізованою інформацією (user, source, localport і reason в разі невдачі):

Значение
18:42:23 2014/02/24 .1.3.6.1.4.1.9.9.41.2.0.1 Normal "Status Events" 192.168.1.14 - clogMessageGenerated SEC_LOGIN 5 LOGIN_FAILED Login failed
18:23:47 2014/02/24 .1.3.6.1.4.1.9.9.41.2.0.1 Normal "Status Events" 192.168.1.14 - clogMessageGenerated SEC_LOGIN 6 LOGIN_SUCCESS Login Suc
18:22:21 2014/02/24 .1.3.6.1.4.1.9.9.41.2.0.1 Normal "Status Events" 192.168.1.14 - clogMessageGenerated SEC_LOGIN 5 LOGIN_FAILED Login failed
18:15:04 2014/02/24 .1.3.6.1.4.1.9.9.41.2.0.1 Normal "Status Events" 192.168.1.14 - clogMessageGenerated SEC_LOGIN 6 LOGIN_SUCCESS Login Suc

Рис. 3.5. Деталізовано інформація з лог-файлів

Налаштування тригера для відображення подій на дашборді:

{192.168.1.14:snmptrap["Status"].regexp(LOGIN_FAILED)}&{192.168.1.14:snmptrap["Status"].nodata(3m)}=0

У поєднанні з попереднім пунктом на дашборді (рис. 3.13) буде інформація ось такого плану:

Узел сети	Проблема	Последнее изменение	Возраст	Инфо	Действия
192.168.1.14	Ошибка авторизации (LOGIN_FAILED)	25 Фев 2014 13:37:00	14с		
192.168.1.14	Успешная авторизация (LOGIN_SUCCESS)	25 Фев 2014 13:41:16	8с		
192.168.1.20	В системе User4	17 Фев 2014 17:01:41	2д 19ч 44м		
192.168.1.13	В системе User1 User2 User7	17 Фев 2014 15:54:28	2д 20ч 51м		
192.168.1.10	В системе User1	17 Фев 2014 14:51:16	2д 21ч 55м		
192.168.1.61	В системе User2	17 Фев 2014 14:41:07	2д 22ч 5м		

Рис. 3.6. Деталізовано інформація з лог-файлів

Аналогічно до вищеописаного наприклад, можна здійснювати моніторинг великої кількості подій, що відбуваються на маршрутизаторах Cisco.

Якщо зауважити, то наведений приклад не буде працювати на продуктах Cisco ASA і PIX, так як там інакше організована робота з логування авторизації.

Ще одним прикладом ми розберемо моніторинг авторизації в JunOS 12.1 для пристроїв Juniper. Але тут не використовуються трапи SNMP, тому як немає підтримки відправки трапів з Syslog повідомлень. Нам знадобиться Syslog сервер на базі Unix, в нашому випадку їм буде той же сервер моніторингу.

На маршрутизаторі необхідно налаштувати відправку Syslog на сервер зберігання:

system syslog host 192.168.1.1 authorization info

Тепер всі повідомлення про авторизацію будуть відправлятися на Syslog сервер, можна звичайно відправляти всі повідомлення (any any). Далі переходимо до Syslog сервера і дивимось tcpdump, чи приходять повідомлення:

tcpdump -n -i em0 host 192.168.1.112 and port 514

12:22:27.437735 IP 192.168.1.112.514 > 192.168.1.1.514: SYSLOG auth.info, length: 106

За замовчуванням в налаштуваннях syslog.conf все що приходить з auth.info має записуватися в */var/log/auth.log*. Далі робимо все аналогічно прикладу з моніторингом входів в Unix.

Залишається тільки налаштувати тригер на дану подію так само, як це було розглянуто в прикладі з авторизацією на Unix сервері.

Таким методом можна відстежувати безліч подій, серед яких такі як: збереження конфігурації пристрою (commit), вхід і вихід з режиму редагування конфігурації (edit) [12].

Звертаючи увагу, що аналогічним способом можна здійснювати моніторинг і на пристроях Cisco, але спосіб з SNMP трапами буде більш швидким і зручним, і виключається необхідність використання в проміжному Syslog сервері.

3.2 Рекомендації щодо застосування системи забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix.

Основне завдання адміністратора системи моніторингу Zabbix - це правильна настройка безпечного доступу, підвищення безпеки системи з використанням додаткових інструментів і наявних методів захисту.

Щоб запобігти несанкціонованого доступу до системи Zabbix необхідно провести превентивні заходи с забезпеченням захисту системи, використовуючи існуючи методи та інструменти захисту системи Zabbix;

1. Адміністрування:

розділіть привілеї облікових записів користувачів в Zabbix, по можливості, зробіть окремий обліковий запис для моніторингу;

ізолюйте Zabbix-сервер від тих компонентів, які зловмисник може використовувати в якості точки входу в корпоративну мережу;

не використовуйте стандартні порти для роботи Zabbix-сервера, за замовчуванням використовується - 10051;

не використовуйте стандартні порти для роботи Zabbix-агента за замовчуванням використовується - 10050;

на Windows ОС, Zabbix-агент запускається як служба, краще зробити для неї окремого користувача, інакше служба буде запущена з параметрами системного облікового запису;

налаштуйте шифрування даних в конфігурції Zabbix-агента;

видаляйте із сервера утиліти, які дозволять зловмисникові швидко прокинути тунель;

використовуйте окремі параметри – для адміністрування, не забувайте періодично змінювати пароль у облікових записів і закривати адміністративну сесію після роботи в веб-інтерфейсі;

налаштуйте аудит подій в Zabbix-сервері, щоб фіксувати і відслідковувати події безпеки;

налаштуйте відправку оповіщення про критичні події.

2. Шифрування:

обов'язково використовуйте шифрування між сполуками: Zabbix-сервер, Zabbix-проксі, Zabbix-агента, zabbix_sender, zabbix_get з використанням TLS протоколу v.1.2, за замовчуванням ці компоненти використовують не захищене з'єднання;

в керуванні і налаштуванні зашифрованими сполуками Zabbix використовуйте:

шифрування на основі RSA сертифікатів;

шифрування на основі PSK;

Обов'язково для підтримки шифрування Zabbix, система повинна бути скомпільована і пов'язана з однією з чотирьох криптографічних бібліотек: OpenSSL;

LibreSSL;

GnuTLS;

Mbed TLS;

використовуйте захищене з'єднання із базою даних MySQL і PostgreSQL за допомогою протокола TLS 1.2.

3. Автентифікація:

налаштовуйте зручний та більш та надійний спосіб для входу в систему;

використовуйте основні методи автентифікації за допомогою: Open LDAP, Active Directory, також є можливість задати глобальний метод автентифікації, використовуючи веб-інтерфейс Zabbix: HTTP та LDAP автентифікація.

Глобальна підтримка шифрування та взаємної автентифікації в Zabbix дає можливість користувачам поступово і вибірково покращувати безпеку компонентів.

4. Плагін Zabbix Threat Control:

використовуйте плагін, як сканер інформаційної безпеки;

відслідковуйте стан серверів в мережі;

використовуйте fix-команду, яка усуне вразливість через невстановлених патчів або старих версій пакетів.

5. Протокол SNMP:

відстежуйте події ІБ на мережевих пристроях Cisco и Juniper;

відстежуйте конфігурацій обладнання, виконання команд на комутаторі / маршрутизаторі, успішну авторизацію та невдалі спроба входу [11].

Отже, застосовуючи зазначені рекомендації ви значно підвищите рівень захисту та надійності розподіленої системи моніторингу Zabbix, тому що загрози безпеки можуть виникнути з помилок конфігурації, а система моніторингу є таким компонентом, неправильним з точки зору безпеки, конфігурація якої може критично вплинути на безпеку всіх компонентів мережі.

ВИСНОВКИ

В роботі досліджено та проаналізовано проблеми забезпечення кібербезпеки інформаційних систем, які є складової частиною функціонування об'єктів критичної IT-інфраструктури, встановлена сутність завдань та реалізація комплексу заходів, спрямованих на вирішення та забезпечення надійності захисту.

Також проаналізовано проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи, визначені засоби та методи щодо реалізації забезпечення комплексного захисту кінцевих точок корпоративної інформаційної системи та рекомендації їх вирішення.

Здійснено аналіз методів та засобів забезпечення кібербезпеки системи розподіленого моніторингу стану корпоративної мережі Zabbix. Визначені основні функції та склад засобів забезпечення кібербезпеки. Проаналізовані новітні методи шифрування, що забезпечують надійний захист між компонентами системи моніторингу Zabbix. Розглянуто стандартні методи автентифікації користувачів за допомогою (Open LDAP, Active Directory), які пропонують розширені опції безпечної автентифікації та гнучку схему доступу користувачів. Також досліджені існуючи методи двофакторної автентифікації користувачів інформаційних систем, які можуть бути ефективно використані та призначені для безпечного та захищеного входу в систему.

В роботі запропоновано варіант розробки технології забезпечення кібербезпеки системи Zabbix із застосуванням двофакторної автентифікації.

Розглянуто існуючи технології забезпечення захисту системи Zabbix корпоративної мережі на основі шифрування, автентифікації, розмежування прав доступу користувачів, використовуючи сторонній плагін Zabbix Threat Control як сканер ІБ. Також за допомогою Zabbix можна ефективно відстежувати події ІБ на мережевих пристроях Cisco и Juniper, використовуючи протокол SNMP.

Таким чином, зазначені рекомендації щодо забезпечення захисту системи розподіленого моніторингу Zabbix корпоративної мережі відповідають всім

вимогам захисту та надійності під час передачі даних всередині корпоративної мережі, в якій відбувається моніторинг подій та сбір величезної кількості інформації. Окрім розподіленого моніторингу основним завданням постає захист та забезпечення системи, спрямований на підвищення рівня захищеності від несанкціонованого доступу збоку зловмисників (хакерів).

ПЕРЕЛІК ПОСИЛАНЬ

1.INDUSTRY TRENDS. The Rise of Security-Driven Networking and the Future of Network Security [Електронний ресурс] – Режим доступу: https://www.fortinet.com/blog/industry-trends/the-rise-of-security-driven-networking-and-the-future-of-network-security

2.What Is Endpoint Security? [Електронний ресурс] – Режим доступу: https://www.trellix.com/en-us/security-awareness/endpoint/what-is-endpoint-security.html

3.The Importance of Endpoint Security [Електронний ресурс] – Режим доступу: https://hyperproof.io/resource/endpoint-security/

4.Endpoint Security Risks - Why It Matters Now More Than Ever [Електронний ресурс] – Режим доступу: https://preyproject.com/blog/endpoint-security-risks

5.Types of Endpoint Security [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/types-of-endpoint-security

6.What is an Endpoint Protection Platforms ? [Електронний ресурс] – Режим доступу: https://www.gartner.com/reviews/market/endpoint-protection-platforms

7.What is Information System? Definition, Examples, & Facts [Електронний ресурс] – Режим доступу: https://emeritus.org/in/learn/information-system/

8.What is an Information System? [Електронний ресурс] – Режим доступу: https://www.mastersindatascience.org/learning/what-is-an-information-system/

9.Zabbix Manual [Електронний ресурс] – Режим доступу: https://www.zabbix.com/documentation/current/en/manual

10.Zabbix Monitoring: The Ultimate Guide [Електронний ресурс] – Режим доступу: https://adamtheautomator.com/zabbix-monitoring/

11.Zabbix: An Introduction To The Server Monitoring Tool [Електронний ресурс] – Режим доступу: https://techblog.geekyants.com/zabbix-an-introduction-to-the-server-monitoring-tool

12.Zabbix Installation and Basic Configuration Guide [Електронний ресурс] – Режим доступу: https://woshub.com/zabbix-install-configure-guide/

13.two-factor authentication (2FA) [Електронний ресурс] – Режим доступу: https://www.techtarget.com/searchsecurity/definition/two-factor-authentication

14.What Is Two-Factor Authentication (2FA)? [Електронний ресурс] – Режим доступу: https://authy.com/what-is-2fa/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)