УДК 004.056
DOI: 10.31673/2409-7292.2021.044450

Лісовий Д.М., Драгунцов Р.І.

УПРАВЛІННЯ ЗАХИСТОМ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПЛАТФОРМІ HCL BIGFIX

В роботі зроблено аналіз проблеми забезпечення кібербезпеки корпоративної інформаційної системи та визначено мета та завдання управління захистом кінцевих точок корпоративної інформаційної системи. Проведено аналіз існуючих технологій управління захистом кінцевих точок корпоративної інформаційної системи. Досліджено методи та засоби управління захистом кінцевих точок на прикладі HCL BigFix. Визначено призначення, основні функції та склад платформи HCL BigFix. На основі досліджень проведених в роботі розроблено варіант технології управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Ключові слова: корпоративна інформаційна система, кібербезпека, захист кінцевих точок.

Вступ

Забезпечення безпеки кінцевих точок в умовах кібервпливів відноситься до методології захисту корпоративної мережі під час доступу через віддалені пристрої, такі як ноутбуки або інші бездротові і мобільні пристрої. Кожен пристрій з віддаленим підключенням до мережі створює потенційну точку входу для загроз безпеки. Зазвичай безпека кінцевих точок забезпечується системою, яка складається з програмного забезпечення безпеки, розташованого на центрально керованому і доступному сервері або шлюзі в мережі, на додаток до клієнтського програмного забезпечення, що встановлюється на кожній з кінцевих точок (або пристроїв). Сервер автентифікує логіни з кінцевих точок, а також оновлює програмне забезпечення пристрою при необхідності. Хоча програмне забезпечення для забезпечення безпеки кінцевих точок розрізняється залежно від постачальника, можна очікувати, що більшість пропозицій програмного забезпечення будуть містити антивірусне та антишпигунське програмне забезпечення, міжмережевий екран, а також систему запобігання вторгнень на хост (HIPS).

Безпека кінцевих точок стає все більш поширеною функцією кібербезпеки корпоративних мереж, оскільки все більше співробітників залучають до роботи мобільні пристрої споживачів, а компанії дозволяють своїм мобільним співробітникам використовувати ці пристрої в корпоративній мережі. Також, застосування технології захисту саме кінцевих точок реалізує принцип «розподіленого захищеного середовища». Це визначає актуальність дослідження щодо управління захистом кінцевих точок корпоративної інформаційної системи на базі HCL BigFix.

Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи. Сьогодні переважна більшість атак на корпоративні ІТ-системи здійснюються зловмисниками через використання проломів і вразливостей кінцевих точок – пристроїв, які використовуються кінцевими користувачами: ПК, ноутбуки, планшети, смартфони тощо. Це є логічним та зрозумілим, беручи до уваги факт того як і ким експлуатуються ці пристрої: велика кількість самих пристроїв, багато доступних каналів зв'язку і портів, розмаїття встановленого ПЗ, не надто висока кваліфікація користувачів, низький рівень їх відповідальності тощо. У результаті кінцеві точки стали найуразливішим місцем будь-якої ІТ-інфраструктури, через яке здійснюється чотири п’ятих всіх атак, з якими пов’язані майже всі шахрайські дії та ненавмисні події інформаційної безпеки.

Як зазначається в [1] кінцеві точки користувачів продовжують залишатися постійною проблемою для організацій. Найбільш успішні зломи кінцевих точок пов'язані з людськими чинниками, такими як соціальна інженерія/фішинг, спроби проникнення через Інтернет і програми-вимагачі. Існує можливість заражень через USB-пристрої в якості початкового вектора атаки. Підкреслюється, що антивірус був найбільш часто використовуваним інструментом для виявлення початкового вектора атаки та тільки 47% атак були виявлені за його допомоги. Інші 32% атак були виявлені за допомогою автоматичних попереджень SIEM

і мережевого аналізу, а 26% були виявлені за допомогою платформ EDR (виявлення кінцевих точок і реагування) [1]. Тільки 23% зломів респондентів були виявлені за допомогою моделювання поведінки атак і тільки 11% зломів за допомогою поведінкової аналітики. Оскільки поведінка користувачів і комп'ютерів є причиною більшості порушень роботи кінцевих точок, ці технології мають вирішальне значення для виявлення кінцевих точок і реагування на них [1].

Однією з проблем є те, що групи безпеки не справляються з задачами з причин коли їх операційний центр безпеки (SOC) завалений такою великою кількістю новітніх інструментів, які б мали скоротити функції кібер-аналітиків, щоб вони могли виконувати аналіз, натомість обмежило їх можливості. для глибокої реалізації або використання доступних опцій [1]. Основними векторами атак на кінцеві точки є веб-сервіси (63%), соціальна інженерія (фішинг) (53%) і програми-вимагачі (50%). Крадіжка облікових даних використовувалася в 40% випадків злому (рис. 1).

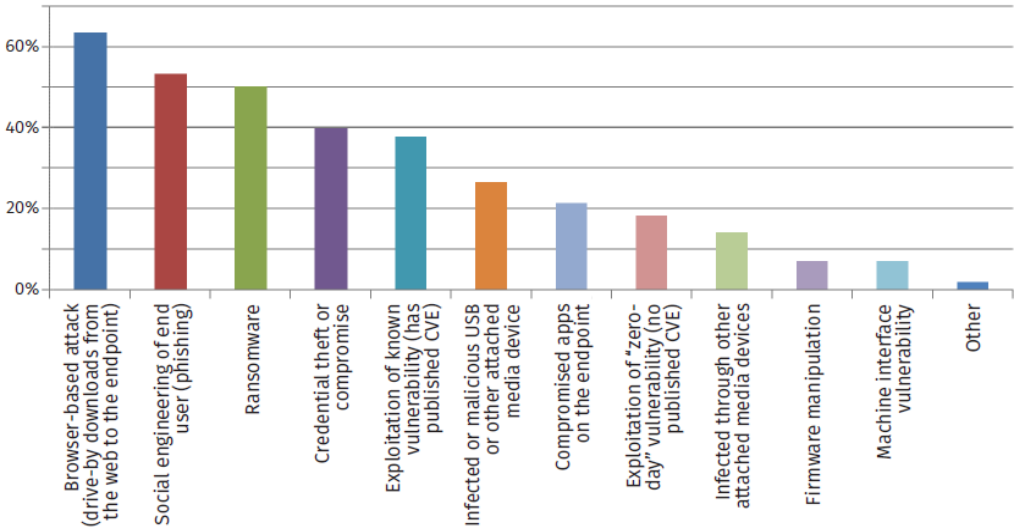

Рис. 1. Вектори атак кінцевих точок [1]

Оскільки основні компрометації залежать від дій користувачів на кінцевих точках, то, відповідно, що операції людини на кінцевій точці повинні контролюватися і стримуватися, а також по можливості треба навчати користувачів. Задля цього треба застосовувати різні інструменти, в тому числі антивірусне програмне забезпечення нового покоління (для виявлення атак без шкідливих програм і файлів) і автоматизований EDR (з антивірусом нового покоління (NGAV), включаючи аналітику поведінки користувачів) [1].

Результати [1] показують, що організації використовують ряд технологій і, ймовірно, централізують пошук за допомогою застосування своїх SIEM-систем. У цих випадках SIEM збирає дані про кінцеві точки і мережеві дані, які організації використовують для пошуку подій, пов'язаних з кінцевими точками, аналізуючи їх за допомогою аналітики кінцевих точок і забезпечуючи кореляцію з елементами даних з систем EDR і інших.

Коли справа доходить до відстеження артефактів для розслідування компрометації, централізований збір даних охоплює багато ключових елементів, такі як інвентаризація та конфігурація ПЗ, але є прогалини [1]:

найбільша прогалина полягає в виявленні резидентних об'єктів в пам'яті, де не працюють антивірус і традиційні механізми безпеки;

виявлення використання конфіденційних даних і відсутність інформації обліку периметру є ключем до розуміння прогалин в охопленні;

респонденти повідомляють, що у них відсутні мережеві дані (між машинного з'єднання і дані протоколу дозволу адрес (ARP)) для кореляції з артефактами кінцевих точок;

у них також відсутні дані про поведінку користувачів, або їх просто не існує.

Щоб переломити ситуацію, організації повинні визначити, встановити й налаштувати ефективні рішення, а також встановити базові показники. Крім придбання інструментів, що забезпечують автоматизацію і функціональну сумісність, організаціям необхідно залучити персонал, необхідний для роботи і використання своїх інструментів, або за рахунок виділення ресурсів, або за рахунок зменшення складності наборів інструментів, з якими аналітики повинні безпосередньо взаємодіяти [1].

Мета роботи – розробити варіант технології управління захистом кінцевих точок корпоративної інформаційної системи та рекомендації щодо застосування технології управління їх захистом на підприємстві.

Архітектура та компоненти платформи HCL BigFix. Щоб організація могла створити стійку стійкість кіберпростору, будуть потрібні деякі аспекти всіх трьох елементів, і створення стійкості кіберпростору буде недешево. Додаткові витрати, понесені тільки на резервування та навчання, перевершать будь-яку потенційну економію від оптимізації і скорочення надлишкових потужностей. Однак, якщо організація серйозно ставиться до захисту своєї здатності виконувати свою місію в кіберпросторі, стійкість буде ключовим фактором [2].

HCL BigFix єдина платформа для управління кінцевими точками, яка дозволяє групам IT і безпеки повністю автоматизувати процеси виявлення, управління та виправлення будь-то локально, віртуально або в хмарі, незалежно від операційної системи, розташування або підключення. На відміну від складних інструментів, які охоплюють обмежену частину корпоративних кінцевих точок і вимагають днів або тижнів на оновлення, BigFix може знаходити і виправляти кінцеві точки швидше, ніж будь-яке інше рішення, при цьому забезпечуючи понад 98% успішних виправлень з першого проходу [3].

Рішення BigFix є багаторівневою технологічною платформою, яка виступає в якості основної частини глобальної IT-інфраструктури. Платформа являє собою динамічну, керовану контентом систему обміну повідомленнями та управління, яка розподіляє роботу з управління IT-інфраструктурою між самими керованими пристроями, агентами. Всі додатки BigFix працюють на платформі BigFix. Платформа може керувати до 250 000 фізичними та віртуальними комп'ютерами в приватних або загальнодоступних мережах, включаючи настільні сервери, портативні комп'ютери в роумінгу, мобільні телефони, пристрої для точок продажів, банкомати та кіоски самообслуговування [3].

Розглянемо основні компоненти архітектури рішення HCL BigFix (рис. 2), функціонування яких реалізує технологію управління захистом кінцевих точок корпоративної інформаційної системи, а саме [3]:

Єдиний інтелектуальний агент повинен бути встановлений на кожному комп'ютері, яким необхідно управляти. Він постійно оцінює стан кінцевої точки відповідно до заявленої політики, незалежно від того, чи підключена вона до мережі чи ні. Як тільки агент бачить, що ціль не відповідає політиці або контрольному списку, він інформує сервер, запускає налаштоване завдання виправлення і негайно повідомляє сервер про стан завдання та його результат. Єдина консоль забезпечує управління кінцевими точками, наприклад, управління захистом кінцевих точок, управління життєвим циклом системи, налаштуваннями безпеки і управління вразливостями та оновленнями.

Єдиний сервер координує потік інформації до окремих клієнтів та від них, зберігає результати в базі даних. Він керує контентом на основі політик і дозволяє оператору підтримувати видимість і контроль в реальному часі над усіма пристроями в середовищі. Контент доставляється в повідомленнях, які називаються Fixlet, і постійно оновлюється за допомогою хмарної служби доставки контенту. Опціональні ретранслятори допомагають керувати розподіленими пристроями і вмістом політик. Ретранслятор – це клієнт, розширений службою ретрансляції. Він виконує всі клієнтські дії для захисту головного комп'ютера і, крім того, доставляє контент і завантаження програмного забезпечення дочірнім клієнтам і ретрансляторам.

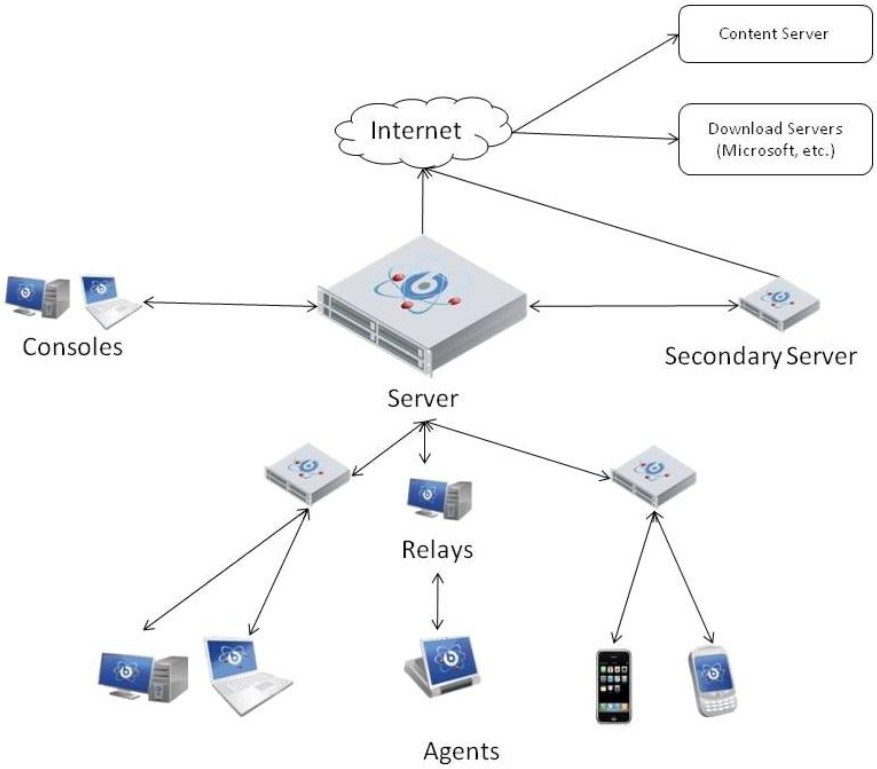

Рис. 2. Основні компоненти архітектури рішення HCL BigFix [3]

Сервер Disaster Server Architecture (DSA) реплікує інформацію сервера для аварійного відновлення. Якщо сервер BigFix виходить з ладу, інші сервери BigFix автоматично стають повністю функціональними серверами BigFix. Додаток Web Reports забезпечує створення діаграм та графіків корпоративних даних, надаючи друковані копії; надає допомогу у веденні контрольного журналу всієї активності Fixlet у корпоративній мережі; забезпечує експорт даних для подальшої обробки в електронну таблицю або базу даних; збирає інформацію з додаткових серверів BigFix; забезпечує роботу інтерфейсу в веб-браузері і надає ряду користувачів можливість бачити стан комп'ютерів без права на зміну цих комп'ютерів.

Таким чином, сучасні підходи базуються на комплексному захисті кінцевих точок корпоративної інформаційної системи, у вигляді клієнта зі всіма необхідними компонентами, що є зручним для кінцевого користувача. Централізоване управління захистом кінцевими точками спрощує роботу адміністраторів безпеки із засобами захисту, так як використовується менше додатків безпеки та, відповідно, витрачається менше зусиль щодо забезпечення їх функціонування.

Варіант технології управління захистом кінцевих точок корпоративної інформаційної системи на базі HCL BigFix. Необхідно зазначити, що HCL BigFix є потужним і багатофункціональним програмним комплексом. Розглянемо приклад робочого процесу оператора консолі HCL BigFix [4].

1. Робочий процес оператора починається із запуску консолі BigFix.

2. На панелі домену необхідно обрати All Content, який дозволяє операторові переглядати всі сайти, на які підписані. Потім необхідно натиснути Fixlets and Tasks у верхній частині панелі Domain. Після цього на панелі списку праворуч відобразиться список Fixlets and Tasks (рис. 3), які в даний час застосовуються до мережі.

3. На панелі списку треба обрати потрібний Fixlet. Відповідний документ відкриється в Робочій області під списком. Це текст Fixlet, який дає операторові інформацію, необхідну для прийняття рішення про розгортання, а також конкретні дії, які необхідно зробити.

4. Внизу повідомлення знаходяться одне або кілька посилань, які ініціюють дії щодо виправлення вразливих комп'ютерів. Необхідно натиснути кнопку дії, яке здається найбільш підходящим. Take Action відкриває діалогове вікно (рис. 4).

5. Оператор може використовувати вкладку Target, щоб вибрати будь-яку підмножина порушених комп'ютерів, на яких він налаштовує відповідні дії.

6. Оператор використовує інші вкладки для підготовки своїх дій, включаючи розклади виконання, клієнтські повідомлення, додаткові сценарії і багато іншого, потім натискає кнопку ОК.

7. Коли оператор вводить свій пароль, дія Fixlet розгортається по всій корпоративній мережі і застосовується спеціально до кожного комп'ютера, який його потребує, з урахуванням всіх встановлених оператором фільтрів.

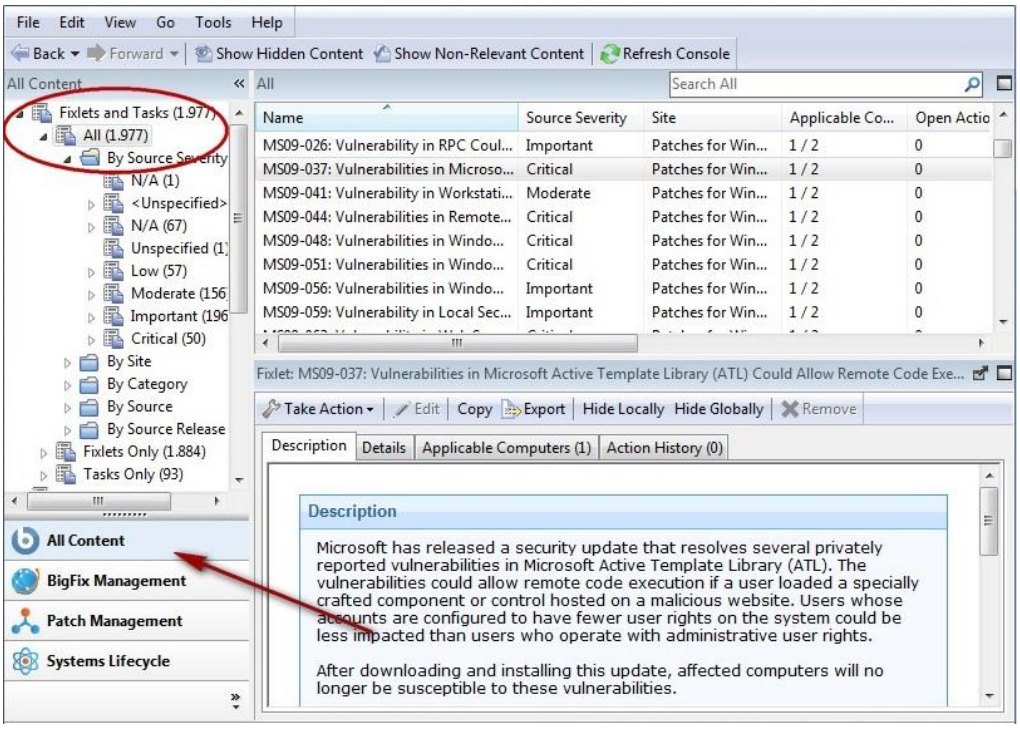

Рис. 3. Список Fixlets and Tasks консолі BigFix

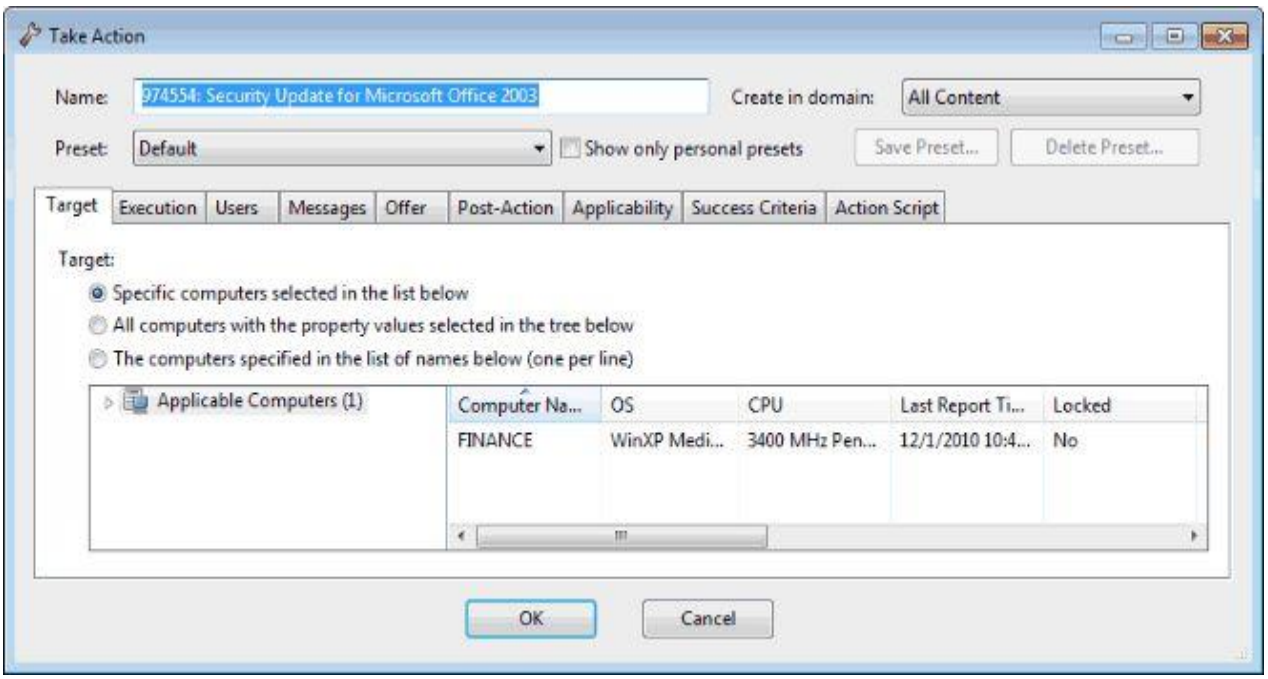

Рис. 4. Діалогове вікно Take Action на консолі BigFix

Розглянутий процес використовує оператор для стандартного обслуговування і виправлення комп'ютера. Вивчивши інтерфейс, оператор виявляє яким чином усувати проблеми безпеки, проводити інвентаризацію комп'ютерів, управляти користувачами і вести докладний контрольний журнал кожного виправлення та оновлення. Якими б різноманітними не були ці завдання, всі вони виконуються схожим робочим процесом.

Рекомендації щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи. За сьогоднішніми стандартами, попередній захист повинен розглядатися як основа будь-якого підходу наступного покоління до захисту кінцевої точки.

Рекомендація: необхідно обирати рішення NGEPP, яке не тільки використовує служби репутації декількох постачальників для попереджувального блокування загроз, а й використовує спрощений метод індексації файлів (пасивне сканування або вибіркове сканування) замість тих, які регулярно виконують ресурсномістке сканування системи. Рішення також повинне забезпечувати функціональність управління додатками. Невідомі загрози (часто ретельно упаковані або змінені варіанти відомих загроз) уникають статичних заходів запобігання і починають виконуватися на кінцевому пристрої. Доцільно застосовувати методи аналізу, засновані на поведінці, що є основою NGEPP. Виявлення складних загроз за допомогою поведінкового аналізу вимагає постійного моніторингу всієї активності на рівні системи на кінцевому пристрої. Такий ступінь моніторингу необхідно для створення контексту нормальної поведінки системи і додатків, що дозволяє швидко виявити серйозну загрозу.

В цілому, виявлення на основі поведінки виявилося набагато більш ефективним, ніж статичне виявлення. Крім того, воно є більш ефективним, ніж інші рішення нового покоління, в яких використовується математичне моделювання для виявлення подібності між структурою підозрілого виконуваного файлу серед різних варіантів і сімейств шкідливих програм. Ці методи, як і раніше обмежуються шкідливими програмами на основі файлів і потрапляють в одну гру в кішки-мишки, коли зловмисники і постачальники засобів безпеки намагаються перехитрити один одного.

Рекомендація: динамічний аналіз поведінки і підхід, який не покладається виключно на попереднє знання конкретного індикатора для виявлення атаки, виявляться більш ефективними при роботі з справжніми атаками нульового дня. Атаки нульового дня рідко відображають будь-які статичні індикатори компрометації, хоча поведінка атаки в значній мірі знайома. Рішення NGEPP може динамічно виявляти загрози нульового дня і складні шкідливі програми без необхідності статичних заходів. Після успішного виконання атаки на одній або декількох кінцевих точках організація залишається вразливою до тих пір, поки співробітники служби безпеки не зможуть повністю пом'якшити її, зупинивши її бічне поширення і видаливши з порушених пристроїв.

Кібератаки часто створюють, змінюють або видаляють системні файли і параметри реєстру, а також вносять зміни в параметри конфігурації. Ці зміни або залишки можуть викликати збої в роботі або нестабільність системи і вимагають значних зусиль для очищення без відповідних можливостей. Багато сучасних технологій орієнтовані на виявлення загрози і оповіщення про неї. Це бентежить персонал, відповідальний за реагування на інциденти, озброєний комбінацією точкових інструментів пом'якшення наслідків і криміналістичної експертизи, а також ручних процедур, за допомогою яких робляться спроби знайти і ізолювати заражені системи. Іноді залучаються експерти-консультанти з безпеки (за значні гроші), коли внутрішнім групам потрібна допомога в усуненні наслідків, виправленні порушених файлів або створенні та інтерпретації даних експертизи. В кінцевому рахунку, найбільш ефективним є відповідь, при якому пом'якшення і усунення атак автоматично виконуються в початковій точці виявлення і ґрунтуються на детальних криміналістичних даних в реальному часі. Найбільш повні рішення для захисту кінцевих точок нового покоління засновані на цілісному підході інтеграції можливостей реагування з виявленням та запобіганням загроз. Це усуває будь-які потенційні проблеми

взаємодії між інструментами безпеки і забезпечує максимально швидкий час відгуку.

Рекомендація: платформа NGEPP повинна підтримувати автоматичне пом'якшення наслідків на основі політик, яке є досить гнучким, щоб охопити широкий спектр сценаріїв використання. Наприклад: карантин заражених файлів, знищення шкідливих процесів, відключення заражених комп'ютерів від мережі або навіть повне відключення скомпрометованих пристроїв. Усунення наслідків повинно виконуватися своєчасно (наприклад, якщо інструменту необхідно зв’язатися з центральним сервером, щоб отримати команду пом'якшення, атака ще може встигнути поширитися вбік). Швидке пом'якшення наслідків на початкових етапах життєвого циклу загрози зведе до мінімуму шкоду і мінімізує необхідних зусиль щодо усунення.

Рекомендація: рішення NGEPP має бути здатним легко виправляти порушені файли, відкочуючись їх до останніх відомих довірених станів.

Рекомендація: рішення NGEPP має забезпечувати повну і детальну видимість того, що сталося на кінцевій точці під час атаки в реальному часі, а також забезпечувати можливість пошуку індикаторів компрометації на кінцевих точках. Дані судової експертизи повинні бути представлені як в інтуїтивно зрозумілому графічному форматі, так і в декількох форматах файлів, сумісних з іншими інструментами безпеки, такими як SIEM.

Таким чином, з огляду на зростаюче розмаїття пристроїв і платформ захисту кінцевих точок в поєднанні з швидко мінливим ландшафтом загроз, захист кінцевих точок стає більш актуальним і важливим, ніж будь-коли раніше. Хоча існує кілька різних підходів і рішень, які підпадають під назву «захисту кінцевих точок наступного покоління», існує чітко визначений набір критичних можливостей і атрибутів, необхідних для реалізації в NGEPP для найкращого обслуговування сучасних корпоративних організацій.

Висновки

В роботі проведено дослідження та аналіз проблеми забезпечення захисту кінцевих точок як складової частини корпоративної інформаційної системи, встановлена сутність завдань їх захисту. Встановлено сутність та зміст управління захистом кінцевих точок корпоративної інформаційної системи. Визначено методи та засоби забезпечення управління корпоративними кінцевими точками, які реалізовані в HCL BigFix. У роботі запропоновано варіант технології управління захистом кінцевих точок корпоративної інформаційної системи на платформі HCL BigFix. для цього було розглянуто приклад робочого процесу оператора консолі HCL BigFix. Розроблено рекомендації фахівцям із кібербезпеки щодо застосування технології управління захистом кінцевих точок корпоративної інформаційної системи на підприємстві.

Таким чином, правильна реалізація технології управління захистом кінцевих точок корпоративної інформаційної системи на платформі HCL BigFix має забезпечити ефективний захист корпоративних даних та кібербезпеку корпоративної інформаційної системи підприємства.

Перелік посилань

1. Misty Blowers. Evolution of Cyber Technologies and Operations to 2035. Advances in Information Security. Springer International Publishing Switzerland 2015. – 201 p.

2. Lee Neely. Endpoint Protection and Response: A SANS Survey. June 2018 [Електронний ресурс] – Режим доступу: https://www.sans.org/reading-room/whitepapers/analyst/endpoint-protection-response-survey-38460.

3. HCL Software. Product Documentation. BigFix [Електронний ресурс] – Режим доступу: https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Getting_Started/c_ibm_endpoint_manager_getting_started.html.

4. HCL Software. BigFix. A sample console operator's workflow [Електронний ресурс] – Режим доступу: https://help.hcltechsw.com/bigfix/10.0/platform/Platform/Console/c_operating_basics.html..

Надійшла: 15.10.2021 Рецензент: д.т.н., професор Вишнівський В.В.