КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.124134
УДК 004.03

Ільєнко Анна Вадимівна
к.т.н., доцент, доцент кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки комп'ютерної та програмної інженерії,
Київ, Україна
ORCID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ільєнко Сергій Сергійович
к.т.н., доцент, доцент кафедри автоматизації та енергоменеджменту
Національний авіаційний університет університет, аерокосмічний факультет,
Київ, Україна
ORCID: 0000-0002-0437-0995
ilyenko.a.v@nau.edu.ua

Куліш Тетяна Миколаївна
бакалавр, студентка кафедри комп'ютеризованих систем захисту інформації
Національний авіаційний університет університет, факультет кібербезпеки комп'ютерної та програмної інженерії,
Київ, Україна
ORCID: 0000-0001-8413-9154
teti98kulish@gmail.com

ПЕРСПЕКТИВНІ МЕТОДИ ЗАХИСТУ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS

Анотація. Стаття присвячена розгляду проблеми забезпечення інформаційної безпеки операційної системи Windows та визначення перспективних методів забезпечення захисту. В даній статті визначено, що базовим підходом щодо безпеки операційних систем виступає процес «загартовування операційної системи». В процесі дослідження наведені статистичні дані поширення популярних операційних систем, а саме Windows, Mac, Linux, Chrome, BSD. Зроблено аналіз та проведено класифікацію сучасних вразливостей операційної системи та на прикладах наведено наслідки їх дії. Дані недоліки можуть спровокувати в комп'ютерній системі цілеспрямоване порушення конфіденційності, цілісності та доступності інформації та системи в цілому. На підставі проведеного аналізу вразливостей визначені основні підходи і методи щодо організації захисту операційної системи. Розглянуто стандартні підходи, а саме використання вбудованих засобів захисту програмного забезпечення, захист Active Directory, віртуалізація для стримування атак. На сьогодні значна увага при забезпеченні безпеки операційної системи приділяється криптографії і принципам мережевої, системної та організаційної та операційної безпеки, включаючи аналіз ризиків та відновлення після аварій. Дані підходи є базовими і входять як складові безпеки у сьогоднішні операційні системи , але наразі використання комплексних підходів є більш дієвим. Швидка реакція на порушення цілісності та доступності операційної системи в поєднання з загартовуванням, ось основний напрями розвитку та удосконалення ОС. Доволі новим підходом, що запропонований в статті для захисту Windows продуктів є використання Blockchain напрямку. Наразі він використовується для перевірки цифрових сертифікатів і можна однозначно сказати, що має потенціал і у інших напрямках забезпечення безпеки операційної системи. В роботі показані власні приклади реалізації Blockchain для перевірки сертифікатів, враховуючи деякі із варіацій перевірок. Приклади реалізовано на Python 3.0. Проведене в статті дослідження перспективних методів та засобів захисту операційної системи дозволяє стверджувати, що використання загартовування системи, є одним з дієвих та комплексних підходів щодо забезпечення інформації безпеки, що дозволить своєчасно виявляти вразливості та своєчасно реагувати на порушення базових властивості операційної системи.

Ключові слова: Windows; операційна система; вразливості; захист; Active Directory; Blockchain.

1. ВСТУП

Постановка проблеми. Загартовування операційної системи (ОС) – один з найважливіших кроків до надійної безпеки інформації. Під поняттям загартовування ОС будемо розуміти, те що при виявленні нових вразливостей у ОС, вони фіксуються і виправляються, свого роду, machine learning, але збоку ОС. По мірі того, як операційні системи розвиваються з плином часу і додаються більше можливостей, загартування потрібно коригувати, щоб не відставати від змін в розвитку технологій ОС. Windows 10 офіційно випущена Microsoft в середині 2015 року, стала настільною платформою номер один у 2020 році після того, як їй вдалося обігнати свою попередницю Windows 7 [1]. Статистичні дані, надані аналітичною компанією NetMarketShare, дають більш докладне уявлення про те, на яких позиціях ОС Windows були в минулому році, і підкреслюється їх зростання протягом 2019 року. Так популярність Windows зросла з 87.43% до 88.14% і наразі займає перше місце на ринку ОС у всьому світі, що становить 88.07%. Поширеність Mac ОС також трохи збільшилась – на 0.05%, у той час, коли рейтинг Linux на ринку навпаки впав на 0.64%. І так, на другому місці на світовій шкалі стоїть Mac ОС із своїми 9.44%, третьому – Linux - 1.87%, четверту позицію займає Chrome ОС - 0.41%. Невідомі ОС набирають 0.20%, BSD – 0.01%. Відмітимо, що дані цифри розглядаються з позиції вибірки тільки операційних систем, що використовуються на сьогодні на персональних комп'ютерах, як державних так і приватних підприємствах, але навіть якщо добавити у список мобільні, консольні і інші варіанти, суть не зміниться – продукти Microsoft надійно закріпили свої позиції. Таким чином, необхідні більш високі вимоги та перспективніші методи захисту ОС ніж це було раніше [2], щоб зловмисники не могли обійти захисні функції та внести злоякісні корективи в функціональні можливості ОС.

Аналіз останніх досліджень і публікацій. Як і у книзі Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Derrick Rountree [3], у даній статті розглядаються загальні коцепції безпеки, включаючи принципи інформаційної безпеки, стандарти, регулювання та дотримання; автентифікація, авторизація та облік; та контроль доступу. Аналіз звітів і публікацій про виявлені вразливості у системі Windows і патчів для їх усунення, висвітлені на офіційних сайті Microsoft дають зрозуміти напрями підвищення забезпечення безпеки операційної системи [4,5,6].

Мета статті. У сучасних умовах виникає необхідність розгляду нових методів і підходів для захисту операційної системи Windows. Аналіз вразливостей, що і досі існують і усуваються патчами Microsoft підтверджують наявність недоліків у системі. Відповідно для виділення подальших перспективним методів захисту операційної системи, буде правильним підходом аналіз традиційних способів захисту даної системи, і розгляд їх у комплексі з новими напрямками безпеки, одним із яких є Blockchain. Технологія Blockchain при використанні направлена на підвищення рівня цілісності і конфіденційність не тільки даних, а транзакцій між користувачами мережі при використанні операційної системи Windows. Наразі Blockchain набирає обертів, уже існують приклади використання даної технології у перевірці цифрових сертифікатів, але перевірка і досі не є повністю інтегрована із системою захисту Windows.

Метою даної статті є дослідження перспективних методів захисту операційної

системи Windows, окреслення основних підходів щодо забезпечення безпеки та визначення нових підходів до забезпечення безпеки операційної системи, а також представлення власної реалізації напрямку Blockchain для захисту Windows реалізованої мовою програмування Python 3.0 з подальшою можливістю її інтегрування в операційну систему. Для досягнення поставленої мети потрібно розв'язати основні задачі: проаналізувати існуючі вразливості ОС Windows; розглянути існуючі підходи та методи щодо захисту ОС; виділити перспективні методи захисту ОС Windows.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Короткий опис вразливостей. Вразливість у комп'ютерній безпеці трактується як неспроможність системи вчиняти супротив реалізації певної загрози чи сукупності загроз.

Уразливості - в ОС або додатку - можуть бути наслідком: програмних помилок (унаслідок помилки в програмному коді можна дозволити комп'ютерному вірусу отримати доступ до пристрою та взяти під контроль); довантажених функцій, патчів; неправильного налаштування і адміністрування ОС [7,8].

Розглянемо деякі з вразливостей, виявлені у 2020 році. 14 січня 2020 року Microsoft випустила виправлення програмного забезпечення для вирішення 49 вразливих місць у рамках щомісячного оголошення Patch Tuesday. Серед виправлених вразливостей були критичні недоліки в Windows CryptoAPI, шлюз віддаленого робочого столу Windows (RD Gateway) та клієнт віддаленого робочого столу Windows. Зловмисник може віддалено використовувати ці вразливості для дешифрування, зміни або введення даних на з'єднання користувачів.

Вразливість підробки CryptoAPI (CVE-2020-060) . Ця вразливість впливає на всі робочі станції, на яких працює 32- або 64-розрядні операційні системи Windows 10, включаючи версії Windows Server 2016 і 2019 **[9]**. Даний тип вразливості дозволяє зловмисникам перевірити сертифікат криптовалюти Elliptic Curve, щоб обійти довіру, дозволяючи шкідливому програмному забезпеченню ховатись під автентичне підписання надійною, довіреною організацією. Це надає можливість перешкоджає виявленню зловмисних програм. Як варіант, може бути створений зловмисний сертифікат для імені хоста, яке його не авторизувало. У такому разі, браузер, який перекидає роботу на Windows CryptoAPI, не покаже попередження і дозволить зловмиснику дешифрувати, змінити або ввести дані для з'єднання користувачів без їх виявлення.

Вразливості клієнта шлюзу Windows RD та віддаленого робочого столу Windows (CVE-2020-0609, CVE-2020-0610 та CVE-2020-0611). Ці вразливості актуальні для Windows Server 2012 та Windows 7 і новіших. Ці вразливості - на клієнтах віддаленого робочого столу Windows та на сервері шлюзу RD - дозволяють виконувати віддалене виконання коду, де довільний код можна було вільно виконувати. Вразливості сервера не потребують автентифікації чи взаємодії з користувачем, і їх можна експлуатувати спеціально створеним запитом. Вразливість клієнта можна використати переконавши користувача підключитися до шкідливого сервера [10,11,12].

3. ПІДХОДИ ТА МЕТОДИ ЩОДО ЗАХИСТУ ОС

На сьогодні безпека ОС ґрунтується на таких ідеях:

1. Надається прямий або непрямий доступ до вмісту ОС. Наприклад, це можуть

бути файли на локальному диску, привілейовані системні виклики, персональні дані власників облікових записів та служби, представлені програмами, що запущені;

2. Можна поділити запити від користувачів, що авторизовані і неавторизовані, надавши доступ, або ж заборонивши його відповідно. Все це реалізовується на рівні ОС.

Запити діляться на типи:

1. Зовнішня безпека (запити із-за меж комп'ютера). Це може бути авторизація з середовища консолі або ж завдяки мережевому з'єднанню. Після введення імені і логіна користувача відбувається реєстрація, що ідентифікує його, або ж таких способів як магнітних карток чи біометричних даних [13].

2. Внутрішня безпека (програми, що працюють). Якщо програма уже увімкнена, то відсутні якісь обмеження. Проте варто відмітити, що вона має унікальний ідентифікатор, щоб перевірити запити до ресурсів [14].

На додачу до моделі дозволити/заборонити системи з підвищеним рівнем безпеки також слідкують за діяльністю користувачів, що дозволяє пізніше дати відповідь на питання типу «Хто читав цей файл?»

Microsoft, захист від ATP Microsoft Defender та різні рішення щодо безпеки Microsoft утворюють єдиний набір систем захисту підприємств до та після порушення, який в основному інтегрується в кінцеву точку, особистість, електронну пошту та програми для виявлення, запобігання, дослідження та автоматичного реагування на складні атаки.

Розглянемо основні підходи і методи, що використовуються сьогодні для захисту Windows:

Використання вбудованих засобів захисту програмного забезпечення.

Microsoft розробила інтерфейс сканування програмного забезпечення antimalware scan interface (AMSI), який може вловлювати шкідливі сценарії в пам'яті. Будь-яка програма може викликати його, і будь-який зареєстрований механізм антивірусного програмного забезпечення може обробляти вміст, поданий на AMSI.

Кіберзлочинці все частіше покладаються на атаки на основі сценаріїв, особливо на ті, які виконуються в PowerShell, в рамках своїх кампаній. Організаціям важко виявити атаки з використанням PowerShell, оскільки їх важко відрізнити від законної поведінки. Також важко відновити, оскільки сценарії PowerShell можна використовувати для порушення будь-якого аспекту системи чи мережі. Практично в кожній системі Windows, що зараз завантажена PowerShell, атак на основі сценаріїв стає все більш поширеним. Злочинці почали використовувати PowerShell і завантажувати сценарії в пам'ять.

Незважаючи на те, що легко виявити скрипти, збережені на диску, не так просто зупинити виконання сценаріїв, збережених у пам'яті. AMSI намагається ловити сценарії на рівні хоста. AMSI не є ідеальним - він менш корисний для виявлення прихованих скриптів або скриптів, завантажених з незвичних місць, таких як простір імен WMI, ключів реєстру та журналів подій. Сценарії PowerShell, що виконуються без використання powershell.exe (такі інструменти, як сервер мережевої політики), також можуть збільшити AMSI. Існують способи обійти AMSI, наприклад, зміна підпису сценаріїв, використання PowerShell версії 2 або відключення AMSI. Незалежно від того AMSI можна і досі вважати «майбутньою адміністрацією Windows».

Захист Active Directory

Active Directory(AD) стає ще більш важливою складовою, оскільки організації продовжують переміщувати свої робочі навантаження в хмару. Більше не

використовується для обробки автентифікації та управління внутрішніми корпоративними мережами, AD тепер може допомогти в ідентифікації та автентифікації в Microsoft Azure [15].

Усі автентифіковані користувачі мають доступ до більшості, якщо не всіх, об'єктів та атрибутів в Active Directory. Стандартний обліковий запис користувача може скомпрометувати весь домен Active Directory через неправильно надані права змінити об'єкти групової політики, пов'язані з доменом та організаційним підрозділом. За допомогою користувацьких дозволів OU людина може змінювати користувачів та групи без підвищених прав, або вони можуть пройти через історію SID, атрибут об'єкта облікового запису користувача AD, щоб отримати підвищені права [16]
.

Стратегії, які допомагають підприємствам уникати поширених помилок, і зводиться до захисту облікових даних адміністратора та ізоляції критичних ресурсів: бути в курсі оновлень програмного забезпечення, особливо патчів, що стосуються вразливих місць ескалації привілеїв; сегментувати мережу, щоб зловмисникам було важче просуватися через бічні сторони.

Фахівці з питань безпеки повинні визначити, хто має права адміністратора на AD та у віртуальному середовищі, де розміщуються віртуальні контролери домену, а також хто може увійти до контролерів домену. Вони повинні сканувати домени активних каталогів, об'єкт AdminSDHolder та об'єкти групової політики (GPO) на предмет невідповідних спеціальних дозволів, а також гарантувати, що адміністратори домену (адміністратори AD) ніколи не входитимуть у ненадійні системи, такі як робочі станції, з їх чутливими обліковими даними. Права на обліковий запис служби також повинні бути обмежені [17].

Віртуалізація для стримування атак

Microsoft представила напрям забезпечення безпеки ОС, який заснований на віртуалізації virtualization-based security (VBS), де набір функцій захисту, запечатаних у гіпервізорі, в Windows 10. Поверхня атаки для VBS відрізняється від інших реалізацій віртуалізації.

Hyper-V має контроль над кореневим розділом, і він може впроваджувати додаткові обмеження та надавати безпечні послуги. Коли VBS увімкнено, Hyper-V створює спеціалізовану віртуальну машину з високим рівнем довіри для виконання команд безпеки. На відміну від інших віртуальних машин, ця спеціалізована машина захищена від кореневого розділу. Windows 10 може забезпечити цілісність коду бінарних файлів і скриптів у режимі користувача, а VBS обробляє код режиму ядра. VBS розроблений так, щоб не дозволяти виконувати жодний непідписаний код у контексті ядра, навіть якщо ядро було порушено. По суті, довірений код, що працює в спеціальному дозволі VM, виконує права на таблиці розширених сторінок кореневого розділу (EPT) на сторінки, що зберігають підписаний код. Оскільки сторінка не може бути одночасно записуваною та виконуваною, зловмисне програмне забезпечення не може перейти в режим ядра таким чином.

Існуюча документація передбачає, що потрібна безпечна завантаження, а VTd і модуль довіреної платформи Trusted Platform Module (TPM) необов'язкові для включення VBS, але це не так. Для захисту гіпервізора від компрометованого кореневого розділу адміністраторам необхідно мати як VTd, так і TPM. Просто ввімкнути Credential Guard недостатньо для VBS. Необхідна додаткова конфігурація для того, щоб облікові дані не відображалися в кореневому розділі.

4. ПОДАЛЬШІ НАПРЯМИ ДОСЛІДЖЕННЯ

Microsoft продовжує експериментувати з цілю покращення безпеки і запроваджує більше варіантів безпеки ОС [18]. Так можливий перехід до випуску всього лиш одного маштабного оновлення для ОС Windows у рік. Всі решта патчів будуть коректувати наявні у ній недоліки по мірі їх виявлення. Перехід на нову схему може відбутись у 2020 р., а перші випробовування вона пройшла у 2019 р.

Подальші напрями дослідження Microsoft спрямовані на пошук перспективних методів захисту операційної системи Windows. Планку безпеки можна підняти за рахунок звернення уваги на класи, що реалізовані через центр безпеки Windows Defender, який забезпечує комплексний захист.

Управління загрозами та вразливістю. Ця вбудована функція використовує підхід, що змінюється на основі тестування, до виявлення, визначення пріоритетності та виправлення вразливості та неправильних налаштувань кінцевих точок [19].

Зменшення поверхні. Атаки набору можливостей для зменшення поверхні атаки забезпечує першу лінію захисту в групі. Забезпечивши правильне налаштування параметрів конфігурації та застосувавши методи пом'якшення експлуатації, цей набір може протистояти атакам та експлуатації. Цей набір можливостей також включає захист мережі та захист веб-сторінок, які регулюють доступ до шкідливих IP-адрес, доменів та URL-адрес.

Захист наступного покоління. Для подальшого посилення периметра безпеки вашої мережі Microsoft Defender ATP використовує захист наступного покоління, призначений для уловлювання всіх типів нових загроз. Встановлено можливості виявлення та реагування на кінцеві точки для виявлення, дослідження та реагування на розширені загрози, які, можливо, пройшли через перші два стовпи безпеки. Розширене полювання забезпечує інструмент полювання на загрозах на основі запитів, який дозволяє вам активно знаходити порушення та створювати власні виявлення.

Автоматизоване розслідування та виправлення. У поєднанні з можливістю швидко реагувати на розширені атаки, Microsoft Defender ATP пропонує автоматичні можливості розслідування та виправлення, які допомагають зменшити обсяг сповіщень за лічені хвилини.

Безпечний рахунок. Безпечний показник тепер є частиною системи управління загрозами та вразливістю як оцінка конфігурації. Сторінка захищених балів буде доступна протягом декількох тижнів. Перегляньте сторінку "Безпечна оцінка".

Microsoft Defender ATP включає захищену оцінку, яка допоможе вам динамічно оцінити стан безпеки вашої корпоративної мережі, виявити незахищені системи та вжити рекомендованих дій для покращення загальної безпеки вашої організації.

Експерти Microsoft Threat Experts. Новий сервіс по керуванню загрозами Microsoft Defender ATP забезпечує активне полювання, встановлення пріоритетів та додатковий контекст та уявлення, які надають додаткові можливості оперативним центрам безпеки (SOC) для швидкого та точного визначення та реагування на загрози [20].

Blockchain напрямок для перевірки сертифікатів.

Класи, що згадані вище уже реалізовані через центр безпеки Windows Defender і мають перспективу у подальшому вивчені і використанні. Напрямком який також вартий уваги і який досі є не повністю інтегрованим у системі Windows є Blockchain. Дана технологія несе у собі підвищення рівня цілісності і конфіденційність не тільки даних, а транзакцій між користувачами мережі. Наразі Blockchain набирає обертів, уже

ISSN 2663 - 4023

існують зразки його використання у перевірці цифрових сертифікатів. Внесок цього напрямку значно підняв би рівень безпеки продукту Microsoft [21].

Blockchain це безперервний послідовний зв'язний список, побудований за певними правилами. Blockchain-розробник створює програмні додатки, які будуть виконуватися вузлами, що входять в ланцюжок блоків. Також він налаштовує взаємодію «класичного» програмного забезпечення, або DApp (Distributed application), з цими додатками. Як приклад наводимо елементи власної реалізації Blockchain який використовується для перевірок серифікатів, і який враховує варіацій перевірок, наведені нижче. Приклад реалізовано на Python 3.0:

Перевірка закінчення терміну придатності. У всіх версіях це є опцією.

```
expired_group = ExpiredChecker(certificate_model.expires)
steps.append(VerificationGroup(steps=[expired_group],
name='Checking certificate has not expired'))
```

Перевірка відкликання. У всіх версіях є таке

```
 revocation_group = create_revocation_verification_group(certificate_model,
issuer_info, transaction_info)
    steps.append(revocation_group)
```

Перевірка справжності

```
  if chain != Chain.mockchain and chain != Chain.bitcoin_regtest:
        key_map = {k.public_key: k for k in issuer_info.issuer_keys}
        authenticity_checker = AuthenticityChecker(transaction_info.signing_key,
transaction_info.date_time_utc, key_map)
        steps.append(VerificationGroup(steps=[authenticity_checker],
                                       name='Checking authenticity'))
    if chain == Chain.mockchain or chain == Chain.bitcoin_regtest:
        return VerificationGroup(steps=steps, name='Validation',
success_status=StepStatus.mock_passed)
    return VerificationGroup(steps=steps, name='Validation')
```

Але окрім кількісного складу перевірок важливу роль грає правильність конфігурацій цих перевірок, наявність exceptions у коді програмного продукту, що дозволяють уникнути непередбачуваних і помилкових ситуацій.

Головне завдання Blockchain-розробника - розробка цифрових «угод» (смарт-контрактів). Умови в них описуються програмно, а отриманий смарт-контракт розташовується в ланцюжку блоків. Це запобігає втручанню в його роботу або зміні його змісту. А значить, відкидається і можливість відхилення від правил, закладених в «угоді».

Тут значну роль грають конектори і їх налаштування. Конектори, що підтримують пошук трансакцій можна реалізувати як через код нижче, так і через абстрактне створення класу.

```
def createTransactionLookupConnector(chain=Chain.bitcoin_mainnet, options=None):
    if chain == Chain.mockchain or chain == Chain.bitcoin_regtest:
        return MockConnector(chain)
    elif chain.blockchain_type == BlockchainType.ethereum:
        if options and 'etherscan_api_token' in options:
            etherscan_api_token = options['etherscan_api_token']
        else:
            etherscan_api_token = ''
        return EtherscanConnector(chain, etherscan_api_token)
```

```
return FallbackConnector(chain)
```

Кількість таких перевірок ,можливих розвитків подій і варіантів рішення, виходу із ситуацій, пропорційна гарантії рівня безпеки не тільки роботі певного модуля, а й цілої системи. Blockchain напрямок активно використовується зараз у цілях безпеки ОС Windows на стороні реалізації програмного продукту.

5. ВИСНОВКИ

Загартовування є важливою частиною інформаційної безпеки, і методи, про які говорилося вище, є лише елементами захисту систем Windows, запропонованими у 2020 році. Популярність Windows також робить її цільовою для шкідливих програм. Більшість нових шкідливих програм націлена на вразливості та незахищені користувацькі практики в операційній системі Windows. Слід зазначити, що не існує одного стандарту загартування, а захист не є бінарним вибором. Те, наскільки загартована система Windows, потрібно розглядати в контексті потреби організації, а також неабиякої кількості здорового глузду. Саме тому найбільш результативним сьогодні вважається комплексний підхід. Виділивши окремо найбільш важливі елементи ОС можна добитись повноцінного захисту системи із повноцінним захистом, найбільш наближеним до ідеального. В статті авторами представлено власну реалізацію використання напрямку Blockchain для захисту Windows реалізованої мовою програмування Python 3.0, який використовується для перевірок серифікатів, з подальшою можливістю її інтегрування в операційну систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Советы Microsoft [Онлайн] Режим доступу: https://www.cnews.ru/news/top/2020-0113_microsoft_predlozhila_400_mln_polzovatelej [10 березня 2020].
[2] Танненбаум, Э. Современные операционные системы. СПб. : Питер, 1040 с., 2006.
[3] Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211 p.,2011.
[4] Artes, N.O., and S.M. Elsakov. “Protection System of Applications on ‘Windows’ Platform on the Basis of Activity Profile.” Journal of Computational and Engineering Mathematics 3, no. 3 (2016): 3–9. https://doi.org/10.14529/jcem160301.
[5] HU, Hong-yin, Feng YAO, and Cheng-wan HE. “Solution of Windows Files Security Protection Based on File System Filter Driver.” Journal of Computer Applications 29, no. 1 (June 25, 2009): 168–171. https://doi.org/10.3724/sp.j.1087.2009.00168.
[6] Küenzlen, Jürgen, Eckehard Scheller, and Hermann Hamm. “Fixing of Windows with Fall Protection / Befestigung von Absturzsichernden Fensterelementen.” Mauerwerk 20, no. 6 (December 2016): 423–444. https://doi.org/10.1002/dama.201600714.
[7] Гордеев, А.В. Операционные системы : учебник для вузов, Питер, 416 с., 2008.
[8] Проскурин, В.Г. Защита в операционных системах, М. : Радио и связь, 192 с., 2014.
[9] CVE ID [Онлайн] Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2020-060 [10 березня 2020].
[10] CVE-2020-0609 [Онлайн]. – Режим доступу: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609 [10 березня 2020].
[11] CVE-2020-0610 Detail [Онлайн]. – Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2020-0610 [10 березня 2020].
[12] CVE-2020-0611 Detail [Онлайн]. – Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2020-0611 [10 березня 2020].
[13] Дейтел, Х.М. Операционные системы. Ч. 2: Распределенные системы, сети, безопасность, М. : Бином, 704 с., 2006.
[14] Дейтел, Х.М. Операционные системы. Ч. 1: Основы и принципы, М. : Бином, 1024 с., 2007.
[15] J.Spealman, K.Hudson, M.Graft, Windows Server 2003: Active Directory Infrastructure. Microsoft Press, pp. 1–8–1–9, 2003.

[16] Berkouwer, Sander. Active Directory Administration,Veeam Software,620 p.,2019
[17] Edge, Charles S., Jr; Smith, Zack; Hunter, Beau. Enterprise Mac Administrator's Guide. Chapter 3: Active Directory, New York City: Apress, 618 p., 2009.
[18] Защита от потери данных конечной точки [Онлайн]. – Режим доступу: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview [10 березня 2020].
[19] Захист за допомогою служби "Безпека у Windows" [Онлайн]. – Режим доступу: https://support.microsoft.com/uk-ua/help/4013263/windows-10-stay-protected-with-windows-security [10 березня 2020].
[20] Microsoft Defender ATP Advanced Threat Protection [Онлайн]. – Режим доступу: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Microsoft_Defender_ATP_Advanced_Threat_Protection [10 березня 2020].
[21] Bitcoin security guarantee shattered by anonymous miner with 51 % network power [Онлайн]. – Режим доступу: https://arstechnica.com/information-technology/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/ [10 березня 2020].

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Ilyenko Anna
Candidate of Technical Sciences, assistant professor , assistant professor of Information Security Systems Department National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID: 0000-0001-8565-1117
ilyenko.a.v@nau.edu.ua

Ilyenko Sergii
Candidate of Technical Sciences, assistant professor , assistant professor of Automation and Energy Management Department National Aviation University of Kyiv, Aerospace Faculty, Ukraine
ORCID: 0000-0002-0437-0995
ilyenko.a.v@nau.edu.ua

Kulish Tatiana
Student Information Security Systems Department
National Aviation University of Kyiv, Faculty of Cyber Security, Computer and Software Engineering, Ukraine
ORCID: 0000-0001-8413-9154
teti98kulish@gmail.com

PROSPECTIVE PROTECTION METHODS OF WINDOWS OPERATION SYSTEM

Abstract. The article deals with the problem of ensuring information security of the Windows operating system and identifying promising security methods. This article identifies that the basic approach to operating system security is the "hardening of the operating system" process. The study presents statistics on the distribution of popular operating systems, namely Windows, Mac, Linux, Chrome, BSD. The analysis and classification of modern vulnerabilities of the operating system is made and the consequences of their action are given in the examples. These deficiencies can cause a computer system to intentionally violate the confidentiality, integrity and accessibility of information and the system as a whole. Based on the vulnerability analysis, the basic approaches and methods for the organization of protection of the operating system are determined. Standard approaches are discussed, namely the use of built-in security software, Active Directory security, and virtualization to deter attacks. Today, much attention is paid to cryptography and the principles of network, system, organizational and operational security, including risk analysis and disaster recovery, to ensure the security of the operating system. These approaches are basic and are a component of security in today's operating systems, but nowadays, using integrated approaches is more effective. A quick response to the violation of the integrity and accessibility of the operating system in combination with quenching, here are the main directions of development and improvement of the operating system. A rather new approach proposed in the article to protect Windows products is to use the Blockchain direction. It is currently used to validate digital certificates and can be said to have potential in other areas of operating system security. This paper shows examples of Blockchain implementation for certificate validation, taking into account some of the variations of validation. The examples are implemented in Python 3.0. The research of prospective methods and remedies of the operating system conducted in the article suggests that the use of system hardening is one of the effective and comprehensive approaches to providing security information, which will allow timely detection of vulnerabilities and timely response to violations of the basic properties of the operating system.

Keywords: Windows; Operating System; vulnerabilities; protection; Active Directory; Blockchain.

REFERENCES

[1] Microsoft Advices [Online]. Available: https://www.cnews.ru/news/top/2020-0113_microsoft_predlozhila_400_mln_polzovatelej [Accessed: 10 march 2020]. (in Russian).
[2] Tannenbaum, E. Modern Operating Systems. SPb. : Peter, 1040 p., 2006. (in Russian).
[3] Derrick Rountree, Security for Microsoft Windows System Administrators Introduction to Key Information Security Concepts, Syngress, 211 p.,2011. (in English).
[4] Artes, N.O., and S.M. Elsakov. “Protection System of Applications on ‘Windows’ Platform on the Basis of

Activity Profile." Journal of Computational and Engineering Mathematics 3, no. 3 (2016): 3–9. https://doi.org/10.14529/jcem160301. (in English).
[5] HU, Hong-yin, Feng YAO, and Cheng-wan HE. "Solution of Windows Files Security Protection Based on File System Filter Driver." Journal of Computer Applications 29, no. 1 (June 25, 2009): 168–171. https://doi.org/10.3724/sp.j.1087.2009.00168. (in English).
[6] Küenzlen, Jürgen, Eckehard Scheller, and Hermann Hamm. "Fixing of Windows with Fall Protection / Befestigung von Absturzsichernden Fensterelementen." Mauerwerk 20, no. 6 (December 2016): 423–444. https://doi.org/10.1002/dama.201600714. (in English).
[7] Gordeev, A.V. Operating Systems: A Textbook for High Schools, Peter, 416 pp., 2008. (in Russian).
[8] Proskurin, V.G. Protection in operating systems, M.: Radio and communications, 192 p., 2014. (in Russian).
[9] CVE ID [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2020-060 [Accessed: 10 march 2020]. (in English).
[10] CVE-2020-0609 [Online]. – Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609 [Accessed: 10 march 2020]. (in English).
[11] CVE-2020-0610 Detail [Online]. – Available: https://nvd.nist.gov/vuln/detail/CVE-2020-0610 [Accessed: 10 march 2020]. (in English).
[12] CVE-2020-0611 Detail [Online]. – Available: https://nvd.nist.gov/vuln/detail/CVE-2020-0611 [Accessed: 10 march 2020]. (in English).
[13] Daytel, H.M. Operating Systems. Part 2: Distributed systems, networks, security, Moscow: Binom, 704 p., 2006. (in Russian).
[14] Daytel, H.M. Operating Systems. Part 1: Fundamentals and principles, Moscow: Binom, 1024 p., 2007. (in Russian).
[15] J.Spealman, K.Hudson, M.Graft, Windows Server 2003: Active Directory Infrastructure. Microsoft Press, pp. 1–8–1–9, 2003. (in English).
[16] Berkouwer, Sander. Active Directory Administration,Veeam Software,620 p.,2019. (in English).
[17] Edge, Charles S., Jr; Smith, Zack; Hunter, Beau. Enterprise Mac Administrator's Guide. Chapter 3: Active Directory, New York City: Apress, 618 p., 2009. (in English).
[18] Endpoint data loss protection [Online]. – Available: https://docs.microsoft.com/ru-ru/windows/security/threat-protection/microsoft-defender-atp/information-protection-in-windows-overview [Accessed: 10 march 2020]. (in Russian).
[19] Protection by service "Windows Security" [Online]. – Available: https://support.microsoft.com/uk-ua/help/4013263/windows-10-stay-protected-with-windows-security [Accessed: 10 march 2020]. (in Russian).
[20] Microsoft Defender ATP Advanced Threat Protection [Online]. – Available: http://www.tadviser.ru/index.php/%D0%9F%D1%80%D0%BE%D0%B4%D1%83%D0%BA%D1%82:Microsoft_Defender_ATP_Advanced_Threat_Protection [Accessed: 10 march 2020]. (in English).
[21] Bitcoin security guarantee shattered by anonymous miner with 51 % network power [Online]. – Available: https://arstechnica.com/information-technology/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/ [Accessed: 10 march 2020]. (in English).