УДК 621.395

Голуб Г.В.,
Сомов С.В., к.т.н., доцент,
Гроза П.М., к.т.н., с.н.с.,
Дегтярьова Л.М., к.т.н., доцент,
Корж Ю.М., старший преподаватель
Полтавський національний технічний університет
імені Юрія Кондратюка

АНАЛІЗ ЗАХИЩЕНОСТІ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS 10

***Анотація**. У статті проведено аналіз елементів захищеності операційної системи Windows 10. Ґрунтовно розглянуті апаратні і програмні засоби та механізми захисту операційної системи та проблеми, які призводять до порушення цілісності даних. Проведена класифікація механізмів безпеки. Проаналізовано процес контролю доступу, який складається із різних компонентів.*

***Ключові слова:** операційна система Windows 10, інформаційні технології, захист інформації.*

Вступ

У міру того, як діяльність все більше залежить від інформаційних технологій, проблеми захисту даних стають все більш актуальними. Загрози втрати конфіденціальної інформації стали звичайним явищем в сучасному комп'ютерному світі. Наявність проблем в системі захисту приводять до порушення цілісності даних, втрати важливої інформації, потрапляння важливої інформації стороннім особам та інше. Кожен збій може паралізувати роботу компанії, банку і призвести до відчутних матеріальних втрат. Тому захист інформації є актуальною при використанні сучасних комп'ютерних технологій.

Основна частина

Windows 10 повною мірою використовує нові апаратні технології, що дозволяє забезпечити захист інформацію від злому і витоку інформації.

Для боротьби з шкідливими програмами і зломом, потрібно забезпечити цілісність програм і обладнання, процесу завантаження операційної системи (ОС) в цілому. До випуску Windows 8 це було пов'язане зі значними труднощами. Шкідливі програми могли заразити пристрій ще до запуску будь-яких засобів захисту і відключити їх. Пристрої, що пройшли сертифікацію для Windows 8 або пізнішої версії, мають новий апаратний компонент UEFI, який допомагає забезпечити цілісність системного програмного забезпечення (ПЗ) і ОС з моменту включення живлення і до його відключення.

Криптографічна обробка. З огляду на реальний ризик спроб злому, є потреба в такому забезпеченні, яке гарантувало б максимальний рівень захисту найбільш конфіденційних відомостей, таких як ключі шифрування і паролів користувачів. Для захисту таких даних використовується довірений платформний модуль. Операції виконуються в апаратному середовищі та ізольовані від ОС. Windows 10 також може використовувати довірений платформний модуль, щоб переконатися, що засоби захисту і забезпечення цілісності працювали правильно і не були незаконно змінені. Завдяки цьому довірений платформний модуль Windows 10 зручно застосовувати в сценаріях віддаленого доступу. Дана технологія знаходить все більшого поширення як в користувацьких, так і в комерційних пристроях і вже є світовим стандартом.

Віртуалізація. Апаратні засоби забезпечення безпеки та ізоляції займають ключове місце в стратегії безпеки платформи. У Windows 10 використовуються технології віртуалізації, які раніше застосовувалися лише в сценаріях для серверів Windows. Використання їх в клієнтському середовищі дозволяє домогтися високого рівня захисту. Безпека на базі віртуалізації реалізується на технології Hypervisor. Вона дозволяє перенести найбільш вразливі процеси Windows в середовище безпечного виконання з метою запобігання їх

незаконної зміни, а також у тому випадку, коли ядро Windows повністю скомпрометовано. У Windows 10 безпеку на основі віртуалізації лежить в основі роботи таких компонентів, як Device Guard і Credential Guard, які відмінно протидіють шкідливому програмному забезпеченні та засобам злому.

Біометричні датчики. Біометрія на платформі і пристроях Windows доступна вже досить давно, проте до випуску Windows 10 вона відносилася швидше до факторів зручності. Такий підхід до введення імені користувача і пароля дозволяв зробити процедуру входу більш індивідуалізованою, проте весь потенціал біометрії щодо перевірки автентичності так і не був реалізований. Але все змінилося з виходом Windows 10 і появою Microsoft Passport і Windows Hello. Ці технології корпоративного рівня надають великі можливості для багатофакторної аутентифікації, яка аналогічна смарт-картам, але при цьому відрізняються більшою гнучкістю завдяки використанню переваг методики розпізнавання відбитків пальця і райдужної оболонки ока.

У Windows 10 реалізовані механізми безпеки, які можна розділити на три групи:

- функції контролю посвідчень і доступу були істотно розширені, щоб спростити процедуру перевірки автентичності користувачів і підвищити її безпеку. До таких функцій відносяться Windows Hello і Microsoft Passport, які краще захищають паролі користувачів завдяки простоті в розгортанні і використанні багатофакторної перевірки автентичності. Ще однією новою функцією є Credential Guard, який використовує систему безпеки на основі віртуалізації (VBS) для захисту підсистем перевірки автентичності Windows і облікових даних користувачів;

- захист інформації в місці зберігання, при використанні і в ході передачі. Крім BitLocker і BitLocker To Go для захисту даних в місці зберігання в Windows 10 реалізоване шифрування на рівні файлів, використовується також і система захисту корпоративних даних, що виконує поділ і ізолювання даних. У поєднанні зі службою Rights Management ця технологія дозволяє зберегти дані зашифрованими на час їхнього передачі мережею підприємства. Windows 10

також забезпечує безпеку даних за допомогою віртуальних приватних мереж (VPN) і IPSec;

- опір шкідливому ПЗ включає архітектурні зміни, які можуть ізолювати ключові системні компоненти і компоненти безпеки і захистити їх від загроз. Кілька нових функцій Windows 10 допомагають знизити ризики, пов'язані з шкідливим ПЗ, включаючи VBS, Device Guard, Microsoft Edge і абсолютно нову версію Windows Defender. Крім того, багато функцій захисту від шкідливого ПЗ з ОС Windows 8.1, включаючи контейнери AppContainer для ізоляції додатків і численні функції захисту ОС при запуску, перенесені в Windows 10 і вдосконалені в новій версії системи.

Контроль доступу. Традиційно контроль доступу це процес, який складається з трьох компонент:

- ідентифікація - користувач вказує своє унікальне посвідчення в комп'ютерній системі з метою отримання доступу до ресурсу, наприклад файлу або принтеру. У деяких визначеннях користувач називається «суб'єкт», а ресурс – «об'єкт»;

- перевірка автентичності - процедура підтвердження зазначеного посвідчення і перевірка того, що суб'єкт дійсно є тим, за кого себе видає;

- авторизація - виконується системою з метою порівняти права доступу суб'єкта, що пройшов перевірку автентичності.

Реалізація цих компонентів істотно зміцнює захист секретних даних від зловмисників. Тільки користувач, який підтвердив свою особу і отримав право на доступ до даних, зможе здійснити доступ. В системі безпеки існують різні ступені перевірки автентичності посвідчень і безліч різних вимог до лімітів авторизації. Забезпечення гнучкості контролю доступу, необхідної в більшості середовищ підприємств, є складним завданням для будь-якої ОС. У таблиці 1 перераховані типові завдання при контролі доступу і відповідні рішення, представлені в Windows 10.

Таблиця 1

Рішення для стандартних завдань в галузі контролю доступу в ОС Windows 10

Завдання контролю доступу	Рішення Windows 10
Організації часто використовують паролі, тому що використовувати альтернативні методи занадто складно і дорого.	Windows Hello на пристроях з підтримкою біометрії і Microsoft Passport значно спрощують MFA.
Користувачі планшетів повинні вводити пароль на сенсорному екрані, тому можуть виникати помилки. В цілому цей метод менш ефективний, ніж введення з клавіатури.	Windows Hello дозволяє безпечно проводити перевірку справжності на основі розпізнавання обличчя
Відділ IT повинен придбати засоби сторонніх постачальників і керувати ними, щоб забезпечити дотримання нормативних вимог до контролю доступу та аудиту.	У поєднанні з ОС Windows Server 2012, динамічний контроль доступу забезпечує можливість гнучкого контролю доступу та аудиту з дотриманням численних вимог регулюючих органів в області безпеки і не тільки.
Користувачам не подобається вводити паролі	Єдиний вхід (SSO) забезпечує можливість одноразового входу по паспорту Microsoft Passport і отримання доступу до всіх ресурсів організації без повторної перевірки автентичності.
Вхід в Windows досить довгий за рахунок затримки між спробами входу і може заблокувати обліковий запис користувача в разі атаки методом підбору.	Якщо на системному диску включений BitLocker і активовано захист від атак методом підбору, Windows може перезавантажити ПК після певної кількості невдалих спроб ввести пароль, заблокувати доступ до жорсткого диска і зажадати від користувача введення 48-значного ключа відновлення BitLocker, щоб запустити пристрій і отримати доступ до диску.

Висновок

Windows 10 - це результат багаторічних зусиль корпорації Майкрософт. Ця операційна система стала важливим досягненням корпорації з точки зору безпеки. Багато з нас до сих пір пам'ятають роки Windows XP, коли атаки на ОС Windows, додатки і дані множилися, як сніжний ком, і перетворювалися в серйозні загрози. Завдяки існуючим платформам і рішеннями забезпечується надійний захист даних.

Посилання

1. *Ромель А.П., Финкова М.А., Матвеев М.Д. Windows 10. Все об использовании и настройках. Самоучитель. /М.: Наука и техника, 2016, 336с.*
2. *Мухутдинов И. Революционная десятка. /М.: Самиздат, 2016, 460с.*

Authors: Galina Golub, Somov Serhii, Groza Peter, Degtyareva Larysa, Korg Yuri

Operating system security analysis Windows 10

Abstract. This article provides a detailed analysis of the security elements of Windows 10.

Keywords: Windows 10 operating system, information technology, information security.

Авторы: Голуб Галина Владимировна, Сомов Сергей Викторович, Гроза Петр Николаевич, Дегтярева Лариса Николаевна, Корж Юрий Николаевич

Анализ защищенности операционной системы Windows 10

Аннотация. В статье проведен детальный анализ элементов защищенности операционной системы Windows 10.

Ключевые слова: операционная система Windows 10, информационные технологии, защита информации.