ІНФОРМАЦІЙНА БЕЗПЕКА ДІЯЛЬНОСТІ У ДИСТАНЦІЙНОМУ ФОРМАТІ

Литвиненко О.В., к.т.н., доц. Горелов Д.Ю.
Харківський національний університет радіоелектроніки,
кафедра КРіСТЗІ, м. Харків, Україна
e-mail: oleksandr.lytvynenko@nure.ua

Abstract. The subject of the study is methods for increasing the level of cybersecurity of user activities in remote mode.

У 2020 р. державні та комерційні компанії по всьому світу були змушені оперативно переводити багатьох співробітників на віддалену роботу, що призвело до масового використання найбільш очевидних заходів захисту – міжмережевого екранування та двофакторної аутентифікації. Таким чином, ігнорувалося багато актуальних загроз безпеці.

1. Загрози перехоплення облікових даних, що вводяться в ізольованому середовищі.

Одним із заходів захисту інформації при організації віддаленої роботи у випадку, якщо співробітник використовує особистий пристрій, є віртуалізація робочих місць та публікація програм на термінальному сервері з подальшою ізоляцією середовища.

Справді, якщо на власному пристрої співробітника буде встановлено шкідливе програмне забезпечення, воно не зможе впливати на робоче середовище або робочі програми.

Однак навіть якщо і для найвіддаленішого підключення використовується альтернативна автентифікація, у разі підключення до віртуалізованого робочого місця (VDI) та термінального додатка (наприклад, за RemoteApp) висока ймовірність того, що програма вимагатиме авторизації за допомогою логіну та паролю. У такому разі шкідливе програмне забезпечення може перехопити натискання клавіш, обчислити коректне поєднання «логін-пароль», і зловмисник вже по іншому каналу зможе отримати доступ до конфіденційних даних.

Для нейтралізації цієї загрози рекомендується використовувати рішення класу Single Sign-On (SSO) спільно з рішеннями альтернативної посиленої аутентифікації. Рішення SSO має бути встановлене на офісних робочих місцях, до яких співробітник підключається з VDI, або на термінальному сервері. Далі для підтвердження аутентифікації в корпоративних додатках система вимагатиме пред'явлення альтернативного фактора аутентифікації, після чого SSO самостійно надасть ресурсу необхідні облікові дані.

Таким чином, на особистій робочій станції навіть за наявності кейлоггера не перехоплюються логіни та паролі, що вводяться.

2. Загрози порушення доступності корпоративних ресурсів.

2.1. Дистанційне блокування облікових даних.

Найчастіше для доступу до корпоративних ресурсів використовуються публічні веб-сервіси, доступні через Інтернет, наприклад, веб-клієнт пошти.

Часто ім'я поштової скриньки збігається з ім'ям доменного облікового запису. Зловмисник може спробувати розгадати пароль шляхом підбору. Для нейтралізації цієї загрози включається блокування облікового запису після кількох невдалих спроб введення пароля.

Однак зловмисник може перебирати паролі для цілеспрямованого блокування доменного облікового запису. Така атака може призвести до часткового паралічу деяких бізнес-процесів.

З метою часткової нейтралізації цієї загрози можна скористатися спеціалізованим рішенням для двофакторної аутентифікації (2FA), наприклад, одноразовими паролями. При цьому навіть якщо здійснюється спроба перебору, буде заблоковано другий аутентифікатор, а не обліковий запис.

Таким чином, співробітник збереже можливість отримання доступу до корпоративних ресурсів, щоправда, лише через альтернативне з'єднання або при локальній роботі.

2.2. Втрата чи поломка захищеного носія ключової інформації.

Виконуючи робочі обов'язки, віддалені співробітники можуть користуватися цифровими сертифікатами, наприклад, для підпису документів або підключення до сторонніх веб-сервісів. При цьому у разі втрати або поломки пристрою з'являється задача його оперативної заміни, яка не зможе бути реалізована, особливо якщо співробітник територіально віддалений від офісу.

Для нейтралізації загрози можна скористатися спеціалізованими рішеннями, що реалізують віртуальну смарт-картку (тобто без зберігання ключової інформації на захищеному пристрої, що знімається).

У такому разі зберігання ключової інформації здійснюватиметься у таких контейнерах: 1) на серверній стороні всі операції з ключами виконуються на сервері; 2) контейнер у спеціалізованому модулі всередині пристрою – Trusted Platform Module.

Використання подібних рішень вважається менш безпечним, ніж знімні захищені апаратні носії, проте ці рішення найбільш гнучкі і підходять для описаної нештатної ситуації. Після заміни ключового носія можна відключити віртуальну смарт-карту.

Таким чином, навіть у разі втрати чи поломки ключового носія простою у бізнес-процесах компанії не буде.

3. Загрози відмовлення від авторства дій, які призвели до інциденту.

3.1. Спірні ситуації у разі збою критичного ресурсу.

За будь-якої роботи з IT-ресурсами з боку привілейованих користувачів завжди існує ризик помилок через людський фактор. Самі дії можуть призвести до збою критичного ресурсу.

Навіть при роботі безпосередньо в приміщенні організації буває складно розібратися, що сталося і хто є відповідальним за збій. У разі віддаленого доступу ситуація ускладнюється багаторазово. Подібні розбори інцидентів не лише негативно впливають на робочу атмосферу, коли відбуваються спроби звинуватити невинних, а й витрачають багато часу фахівців на непродуктивні дії.

Використання SIEM дозволить дізнатися, хто підключався до ресурсу, але навряд чи дозволить точно визначити відповідального, не кажучи вже про відсутність даних про послідовність дій, які спричинили збій.

Однак при використанні рішень класу Privileged Access Management (PAM) всі підключення привілейованих користувачів до критичних ресурсів фіксуються у різних форматах (відео- та текстовий запис, знімки екрана, натискання клавіш, передані файли). Далі, використовуючи записи дій, можна оперативно визначити, яка послідовність дій призвела до збою, виявити відповідального за інцидент і визначити чинник навмисності.

3.2. Спроба уникнути відповідальності.

Бувають ситуації, коли в компанії працює інсайдер – внутрішній зловмисник, який цілеспрямовано здійснив дії, що спричинили збій або порушення роботи критичного ресурсу. Саме собою завдання виявлення відповідального вже є складним, проте з допомогою рішення класу PAM можна оперативно знайти винного.

При спробі притягти співробітника до відповідальності, він може сказати, що у нього були вкрадені відповідні дані для доступу до його облікового запису. Ні для кого не секрет, що парольна автентифікація дуже вразлива для загрози розголошення, а сам факт розголошення може бути виявлений після інциденту.

Очевидно, що в такій ситуації будь-який керівник може замислитися про те, що співробітник справді невинний, а те, що сталося, – просто невдалий збіг обставин.

Для нейтралізації цієї загрози рекомендується спільно з рішенням PAM використовувати рішення для 2FA співробітників. Тоді, якщо співробітник дійсно є інсайдером і мав місце інцидент, йому буде важко уникнути відповідальності. Якщо все-таки співробітник заявить, що у нього вкрали телефон, на якому стоїть генератор одноразових паролів, йому буде поставлене логічне запитання: "Чому ви оперативно не повідомили про це службу безпеки?"