

Перевірте, хто має доступ до пошти Microsoft 365

Сторонні застосунки можуть роками читати пошту й файли компанії, навіть якщо ними вже не користуються.

ЩО ВСЕРЕДИНІ

- ☐ 6 перевірок доступу для ІТ
- ☐ Готове повідомлення для ІТ або підрядника
- ☐ Дії при зломі та аркуш рішень

Для: Власники, керівники, ІТ-відповідальні та фінансові працівники українських компаній



Останні 2 сторінки для друку



Veiltrack

Незалежне тестування безпеки

Ситуація

Компанія підключила резервне копіювання пошти. Сервісом уже не користуються, але застосунок міг зберегти окремий доступ до Microsoft 365.

У жовтні 2026 року повідомили про атаку через ConnectWise Cloud Backup із використанням даних для входу застосунку та раніше наданих прав. За даними Huntress, постраждали щонайменше 162 середовища Microsoft 365. Це не стосується автоматично всіх сторонніх застосунків.

Власник погоджує зміни, ІТ перевіряє доступ. Заповнюйте аркуш для кожного застосунку.

01 / 06

Знайдіть сторонні застосунки

Відкрийте Entra → Enterprise applications. Звірте застосунки із сервісами компанії. Запишіть невідомі.

Застосунок має доступ, але ніхто не знає, хто його підключив.

→ ІТ записує назву, ідентифікатор і з'ясовує, хто підключив застосунок.

02 / 06

З'ясуйте призначення застосунку

Запитайте відділ або підрядника, хто користується застосунком, навіщо й коли востаннє.

Ніхто не пояснює призначення застосунку, хоча доступ залишився.

→ Власник призначає відповідального за з'ясування призначення та наслідків відключення.

03 / 06

ВИСОКИЙ РИЗИК

Перевірте права на дані

Entra → Enterprise applications → Permissions.

Перевірте права на читання й зміну пошти та файлів. Запишіть зайві.

Застосунок може читати чи змінювати непотрібні йому дані.

→ Відповідальний підтверджує потреби. ІТ прибирає погоджені зайві права й тестує сервіс.

04 / 06

ВИСОКИЙ РИЗИК

Перевірте права адміністратора

Entra → Roles and administrators. З'ясуйте, чи можуть застосунки керувати поштою або сервісами.

Застосунок керує Microsoft 365 без зрозумілої причини.

→ ІТ перевіряє призначення, погоджує видалення зайвих прав і перевіряє результат.

05 / 06

ВИСОКИЙ РИЗИК

Перевірте входи застосунків

Entra → Sign-in logs → Service principal sign-ins.
Звірте час і джерела входів зі звичайною роботою.

Застосунок входив із невідомого джерела без пояснення відповідального.

→ ІТ перевіряє входи. За підтвердженого стороннього використання негайно обмежує доступ.

06 / 06

Підготуйте припинення доступу

Запитайте ІТ, як припинити доступ і чи постраждають резервні копії, відновлення пошти або інші сервіси.

Невідомо, як припинити доступ і які сервіси зупиняться.

→ Власник погоджує планову зміну. ІТ виконує її за потреби й перевіряє результат.

Що робимо після перевірки застосунку?

Залишити

Відповідальний підтверджує потребу. ІТ перевіряє права й доступні входи. Власник погоджує використання та наступну перевірку. Запишіть, хто ухвалив рішення.

Змінити права

Відповідальний визначає потрібні права. Власник погоджує зміну. ІТ прибирає зайві права підтримуваним способом, тестує сервіс і фіксує результат.

Що робимо після перевірки застосунку?

Відключити

Власник погоджує відключення після перевірки залежностей. ІТ припиняє доступ, перевіряє залишкові підключення й роботу сервісів. Запишіть дату й результат. За підтвердженого стороннього використання обмежуйте доступ негайно.

Не знаю, потрібне рішення

Власник призначає відповідального й строк рішення. ІТ фіксує права та доступні входи. Не розширюйте доступ до з'ясування причин. Підтверджене стороннє використання потребує негайної реакції.

Що переслати ІТ-відповідальному або підряднику

«Покажіть сторонні застосунки з доступом до пошти й файлів Microsoft 365. Для кожного вкажіть користувачів, призначення, права та незрозумілі входи. Виділіть невикористовувані застосунки. Запропонуйте рішення, відповідального й дату виконання.»

ЧОГО НЕ РОБИТИ

Не відключайте потрібні сервіси без перевірки залежностей. За підтвердженого стороннього використання обмежуйте доступ негайно.

● ДІЙТЕ ОДРАЗУ

Як діяти за стороннього використання застосунку

- 1** ІТ негайно обмежує підозрілий доступ, не затримуючи захист заради записів.
За підтвердженого стороннього використання або переконливих ознак злому.
- 2** ІТ зберігає доступні журнали входів, права й час виявлення.
Якщо записи доступні. Не затримуйте обмеження доступу.
- 3** Повідомте власника й відповідального за сервіс про підтверджені сторонні дії.

● ДІЙТЕ ОДРАЗУ • 2/2

Як діяти за стороннього використання застосунку

- 4 ІТ перевіряє зміни прав адміністратора та сторонній доступ до пошти й файлів.
За наявності відповідних даних і записів.
- 5 ІТ замінює ненадійні дані для входу, перевіряє залишковий доступ і відновлює перевірені підключення.
Якщо злам підтверджено або дані для входу ненадійні.

Обмеження доступу не усуває наслідків. Перевірте витік даних і повноту журналів.

Заповніть

Роздрукуйте й заповніть ручкою. Один бланк на один застосунок чи випадок.

Застосунок

Хто користується й навіщо

Доступні дані та права

Права адміністратора Microsoft 365

Результат перевірки входів

Рішення власника

Виконавець і строк

Підтвердження результату

Хто має доступ до вашої пошти Microsoft 365?

Роздрукуйте й роздайте відділу. 30 днів тримайте перед очима й позначайте день, коли діяли за пам'яткою. Коли це стане звичкою, аркуш можна зняти.

Оновлюйте аркуш для нових, невикористовуваних застосунків або після зміни ІТ-підрядника:

- ☐ Звіряю підключені застосунки із сервісами компанії.
- ☐ З'ясовую, хто користується застосунком і навіщо.
- ☐ Перевіряю, які дані застосунок може читати чи змінювати.
- ☐ Перевіряю, чи можуть застосунки керувати Microsoft 365.
- ☐ Перевіряю входи та записую період перевірки.
- ☐ Знаю, як припинити доступ і що перевірити.

30 ДНІВ ДО ЗВИЧКИ: ПОЗНАЧТЕ ДЕНЬ

	Пн	Вт	Ср	Чт	Пт
ТИЖДЕНЬ 1	☐	☐	☐	☐	☐
ТИЖДЕНЬ 2	☐	☐	☐	☐	☐
ТИЖДЕНЬ 3	☐	☐	☐	☐	☐
ТИЖДЕНЬ 4	☐	☐	☐	☐	☐

Ім'я, відділ:

Старт:

Питання щодо безпеки?

Напишіть нам



Vlad Kraevsky

засновник Veiltrack

WEB

veiltrack.io

EMAIL

vlad@veiltrack.io

