Секція 1

ДОСЛІДЖЕННЯ АСПЕКТІВ БЕЗПЕКИ В AZURE COGNITIVE SERVICES

Боровик В.Ю.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник Орєхов О.О.

Актуальність. Останнім часом, автоматизації піддається все більше аспектів життя. Складальні лінії заводів та фабрик в наш час повністю автоматизовані, лише невелика кількість людей підтримує їхню безперебійну роботу. Використання таких ресурсів економить час, трудові ресурси. Крім того, підвищується якість продукції. В наші дні, автоматизація та штучний інтелект дістались навіть таких аспектів як аналіз тексту, його переклад на різні мови та визначення емоційного забарвлення написанного абзацу, речення чи розділу. З іншої сторони, безпеку слід вважати першочерговим пріоритетом при розробці будь-яких програм, а з появою програм з підтримкою штучного інтелекту безпека стає ще важливішою. Саме Azure Cognitive Services вирішують як проблеми з наданням доступу до штучного інтелекту, так і з їх безпекою. Azure Cognitive Services включають різноманітні служби штучного інтелекту, які дозволяють створювати когнітивні рішення, які можуть бачити, чути, говорити, розуміти і навіть приймати рішення.

Метою даної роботи є дослідження безпеки служб Azure Cognitive Services

Основні положення. Служби Azure Cognitive Services підтримують такі аспекти безпеки, як використання безпеки транспортного рівня, аутентифікація, безпечне налаштування конфіденційних даних і Customer Lockbox для доступу до даних клієнтів. Безпека транспортного рівня. Усі кінцеві точки Cognitive Services, доступні через HTTP, застосовують TLS 1.2. З примусовим протоколом безпеки споживачі, які намагаються викликати кінцеву точку Cognitive Services, повинні дотримуватися цих вказівок:

1. Клієнтська операційна система (ОС) повинна підтримувати TLS 1.2;
2. Мова (і платформа), які використовуються для здійснення виклику HTTP, повинні вказати TLS 1.2 як частину запиту.

Аутентифікація. Деякі з пропозицій Cognitive Services включають контроль доступу на основі ролей (Azure RBAC). Azure RBAC можна використовувати, щоб спростити деякі церемонії, пов'язані з ручним керуванням принципалами. Безпечне налаштування конфіденційних даних. Для виконання цього аспекту Azure має підтримку змінних середовища, які виступають більш безпечною альтернативою використанню жорстко закодованих значень для конфіденційних даних. Customer Lockbox для Azure надає клієнтам інтерфейс для перегляду, схвалення або відхилення запитів на доступ до даних клієнтів. Він використовується у випадках, коли інженер Microsoft потребує доступу до даних клієнта під час запиту на підтримку.

Висновки. Azure Cognitive Services підримують багатогранні та зірзнорівневі аспекти безпеки, які, в большості, надаються разом зі службами. Отже, при використанні готового рішення штучного інтелекту від компанії Microsoft, не слід нехтувати такими можливостями, як використання безпеки транспортного рівня, аутентифікація, безпечне налаштування конфіденційних даних і Customer Lockbox для доступу до даних клієнтів.

Список літератури

1. Azure Cognitive Services: Exploring Cognitive Vision. *Towards Data Science*. URL – https://towardsdatascience.com/azure-cognitive-service-computer-vision-33ba62ce9d7e (дата звертання: 20.11.2021);

2. TLS Basics. *Internet Society*. URL – https://www.internetsociety.org/deploy360/tls/basics/ (дата звертання: 20.11.2021);

3. Authenticate requests to Azure Cognitive Services. *Microsoft*. URL – https://docs.microsoft.com/en-us/azure/cognitive-services/authentication (дата звертання: 20.11.2021);

4. Customer Lockbox for Microsoft Azure. *Microsoft*. URL – https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview (дата звертання: 20.11.2021);

5. Braband J., Schäbe Kh. On safety assessment of artificial intelligence. Dependability. 2020;20(4):25-34.

Відомості про авторів

Боровик Вадим Юрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 099-100-51-01, v.borovyk@student.csn.khai.edu

Орєхов Олександр Олександрович, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, к.т.н., професор, a.orehov@csn.khai.edu