Поява концепції Open Banking — це панацея?

І чи потрібний захист даній технології?

Відкритий банкінг робить наше життя зручнішим, але сам потребує захисту. Євгеній ПЕДЧЕНКО, Head of IS Department, Seeton, розповідає про те, як убезпечити цю технологію від кібератак.

Говорячи про розвиток технологій та сервісів в інтернет-банкінгу в Україні, ми можемо спостерігати тенденцію переходу клієнтів від обслуговування у відділеннях до вирішення питань щодо кредиту, переказу коштів чи оформлення картки через смартфон. Так це і відбувалося, коли ще у 2015 році тільки розпочав набирати обертів інтернет-банкінг, який надав можливість клієнтам, перебуваючи вдома, робити перекази коштів чи поповнювати рахунки мобільних операторів, а станом на зараз, на 2025 рік — ми у власному смартфоні маємо можливість відкривати дебетові картки, перераховувати кошти між ними, купувати валюту, не виходячи із дому, чи оновлювати власні персональні дані, не стоячи в черзі у відділенні в спекотні дні.

Open Banking: переваги і ризики

Саме з розвитком даних можливостей ще у 2018 році у Європейському Союзі почала набувати поширення концепція відкритого банкінгу (Open Banking), яка виникла в результаті прогресу цифрових технологій та потреби в більшій фінансовій прозорості та доступності банківських сервісів для користувачів. Першу ініціативу було запроваджено в ЄС в рамках Директиви PSD2 (Payment Services Directive 2), яка зобов'язала банки надати доступ до платіжної інформації третім сторонам через відкриті інтерфейси (API), забезпечуючи безпечний обмін даними для різноманітних фінансових послуг. Це дозволило створити конкуренцію на ринку фінансових послуг, що сприяє інноваціям і полегшує доступ до кредитів, інвестицій та інших фінансових інструментів.

Open Banking дає споживачам більшу свободу вибору та контролю за своїми фінансами. Завдяки цій технології вони можуть централізовано отримувати послуги від різних фінансових установ: банків, кредитних спілок та інших, — через використання єдиної платформи. Це сприяє зниженню витрат та часу на використання різними сервісами, підвищенню зручності та доступу до більш персоналізованих фінансових послуг, таких як автоматичне управління витратами або порівняння умов кредитів і депозитів.

Таким чином, Open Banking є важливим кроком до модернізації фінансових систем, що сприяє зростанню конкурентоспроможності, підвищенню ефективності та зручності для клієнтів різних банківських установ.

То як же захищати Open Banking від кібератак?

Попри вказані переваги, які надає Open Banking, дана інновація також має низку проблем з точки зору кібербезпеки. Оскільки відкриті банківські дані передаються через API і надаються стороннім постачальникам фінансових послуг, це збільшує кількість потенційних точок доступу та вразливостей, через які зловмисники можуть спробувати проникнути в банківську систему, яка надає дану послугу. Через це можуть виникнути проблеми з безпекою, такі як:

- ризик витоку персональних даних клієнтів;
- проблеми з ідентифікацією та авторизацією;
- інтеграція зі сторонніми фінансовими установами;
- кібератаки на API інтерфейси та витік токенів авторизації;
- наявність внутрішніх інсайдерів в зовнішніх фінансових установах тощо.

Концепція Open Banking надає величезні можливості для інновацій у фінансовому секторі, але водночас збільшує ризики в області кібербезпеки. Тому важливо забезпечити належний рівень захисту даних, впровадити новітні механізми автентифікації, моніторинг API та підвищення безпеки персональних даних клієнтів фінансових установ.

Варто зауважити, що, відповідно до дослідження компанії Akamai, протягом 2024 року 84% респондентів зафіксували веб-атаки, пов'язані саме з API-інтерфейсами компаній. Ці атаки завдавали збитків у США на суму в середньому близько $600 тис., у Великій Британії — $500 тис., у Німеччині — $450 тис. тощо.

Саме тому для вирішення перерахованих вище ризиків в інформаційній безпеці рекомендується використовувати рішення Akamai API Security.

Комплексний підхід до захисту API від кібератак

Рішення Akamai API Security (раніше відоме як Noname Security) є інструментом, призначеним для захисту API-інтерфейсів в реальному часі, що є критично важливим для Open Banking та інших цифрових екосистем, де обмін даними між різними платформами стає ключовим аспектом функціонування саме з використанням неконтрольованих API-інтерфейсів. Це рішення допомагає вирішити проблеми кібербезпеки, пов'язані з Open Banking (**рис. 1**).

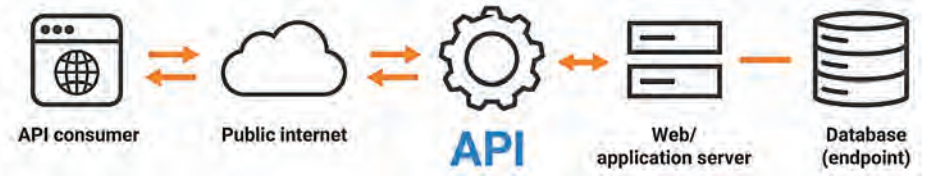

Рис. 1. Принцип роботи API-інтерфейсу в Open Banking

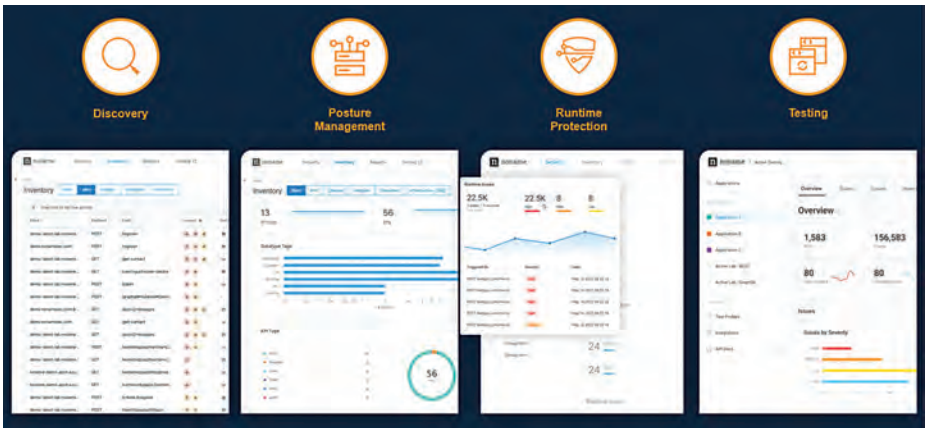

Рис. 2. Комплексний захист від Akamai API Security

1. Захист API від кібератак. Akamai API Security надає можливість виявляти та блокувати шкідливі запити до API ще до того, як вони потраплять до Origin-сервера чи бази даних, і включає захист від атак типу SQL Injection, Cross-Site Scripting (XSS), а також від DoS/DDoS атак.

2. Ідентифікація та управління доступом. Akamai API Security забезпечує чітке управління доступом на рівні кожного API. Система підтримує інтеграцію з такими механізмами, як OAuth та OpenID Connect, що дозволяє налаштовувати безпечний доступ до банківських даних для третіх сторін та користувачів.

3. Моніторинг та аналіз трафіку. Akamai API Security надає комплексне рішення для моніторингу API на предмет загроз і вразливостей. Це дозволяє відслідковувати аномальну поведінку, а також виявляти потенційні проблеми з налаштуваннями безпеки, такі як використання ненадійних веб-джерел чи порушення попередньо налаштованих політик доступу.

4. Захист від витоку конфіденційних даних. Рішення фіксує і контролює будь-які спроби несанкціонованого доступу до банківських даних або їх передачу через API-інтерфейси, що є критично важливим для забезпечення конфіденційності та захисту банківської таємниці.

5. Покращена видимість та звітність. Akamai API Security дозволяє отримувати детальні звіти та аналітику щодо використання кожного API-інтерфейсу. Це важливо для виявлення та розслідування інцидентів безпеки, а також для відповідності міжнародним стандартам та регламентам (наприклад, PCI DSS, GDPR або PSD2).

Рішення Akamai API Security забезпечує комплексний підхід до захисту API, поєднуючи чотири ключові компоненти (**рис. 2**):

- **Discovery** – відповідає за повну інвентаризацію API-активів, виявлення змін тощо;
- **Posture Management** – включає контроль конфігурацій, виявлення та управління вразливостями та пріоритезаціями їх усунення;
- **Runtime Protection** – в режимі реального часу виявляє та блокує кібератаки, а також підозрілу поведінку сервісу;
- **Testing** – дозволяє перевірити безпеку API на етапі розробки й усунути виявлені вразливості до запуску API-інтерфейсу у продуктів.

Akamai API Security пропонує три гнучкі варіанти розгортання, що дозволяють врахувати потреби різних організацій та технічні вимоги (**рис. 3**). Перший варіант — **SaaS** — це повністю хмарне рішення, при якому платформа API Security управляється Akamai в хмарному середовищі. Другий варіант — **Hybrid** — передбачає розміщення віддалених модулів (remote engines) у власному середовищі замовника: наприклад, у датацентрі або приватній хмарі. Третій варіант — **On-Prem** — передбачає повне розгортання платформи, включно з бекендом, користувацьким інтерфейсом та управлінням API, у датацентрі або хмарі замовника, забезпечуючи максимальний контроль над інфраструктурою компанії.

Якщо ваша компанія планує впровадити або вже використовує технологію Open Banking, Akamai API Security є необхідним рішенням для забезпечення надійного захисту вашої банківської таємниці та безпеки API-інтерфейсів. Гарантія безпечного використання Open Banking неможлива без ефективного захисту API, оскільки відкрита передача даних про клієнтів чи рахунки клієнтів і компанії несе за собою ризики кібербезпеки. Akamai API Security надає комплексний захист, який включає виявлення та усунення вразливостей, контроль конфігурацій, моніторинг у реальному часі та активний захист від кібератак. Гнучкі моделі розгортання рішення дозволять вашій компанії легко та швидко адаптувати систему до своєї інфраструктури, гарантуючи максимальний контроль і безпеку даних компанії та клієнтів, що передаються по API-інтерфейсах. Саме тому Akamai API Security є незамінним інструментом для успішного й безпечного використання можливостей технології Open Banking.

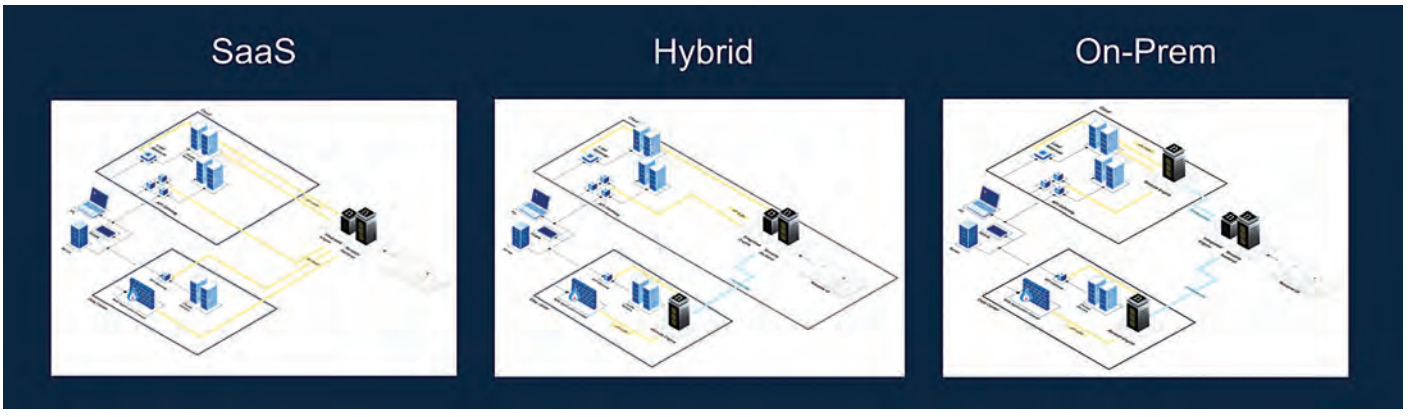

Рис. 3. Варіанти розгортання рішення Akamai API Security

Якщо Вас зацікавило рішення Akamai API Security та Ви бажаєте дізнатися про нього більше або навіть організувати пілотне тестування (Proof-of-Concept) — з цим допоможе компанія **Seeton**, *яка має в своєму складі кваліфікований інженерний склад відділу інформаційної безпеки та найвищий рівень партнерського статусу —* ***Select*** *— по вендору* **Akamai** *серед партнерів України та Азербайджану. Щоб зв'язатися з нами, можна написати на електронну адресу cs@seeton.pro або зателефонувати за номером: +38 044 239 99 99.*