Короваєва Б. М., студентка, гр. ЗКБ-17
Науковий керівник: Пірог О.В., канд. техн. наук,
доцент кафедри КІ та КБ
Державний університет «Житомирська політехніка»

ДЕЯКІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ БІЛІНГУ

В XXI столітті складно переоцінити вплив Internet технологій на життя людей. Online послуги (сервіси) набувають все ширшого розповсюдження. 2020-й рік, завдяки коронакризі, особливо цьому посприяв. Не всі онлайн послуги є безкоштовними. Наприклад, сам доступ до всесвітньої мережі є платною послугою, що надається ISP (Internet Service Provider). Для керування доступом ISP використовує системи білінгу. Подібні системи використовуються і в управлінні доступом до будь-якої online послуги. Наразі білінг розглядається як система контролю і обліку надання платної online послуги провайдером (merchant) клієнту (buyer).

Білінг має наступну структуру:

1. Веб-інтерфейс

- Публічна частина. Вона доступна всім. Веб-інтерфейс містить опис послуги, що надається, рекламні матеріали, умови користування послугою, контакти для зв'язку зі службою підтримки.

- Клієнтська частина.

Доступна тільки клієнтам. Містить дані клієнта, список його платежів, поточний тарифний план, функції з управління: зміна тарифного плану, припинення користуванням послуги, зміна облікових даних.

- Панель керування.

Доступна операторам. Дозволяє керувати тарифами, працювати з клієнтами, отримувати фінансову звітність тощо. Використовуються різні права для різних адміністраторів.

2. Система Управління Базами Даних (СУБД).

Доступна програмним модулям білінгу. Містить дані про тарифи, клієнтів, платежі.

3. Репозиторій.

Репозиторій використовується для зберігання ключів шифрування, паролів, сертифікатів та іншої критично важливої інформації. Репозиторієм може бути файлова система, СУБД, якийсь сервіс. Будь-яка людина за певної умови може стати клієнтом, тобто почати користуватися послугою. Для цього потрібно виконати певні дії. Як правило, це реєстрація і початковий платіж. Іноді ці дії виконуються одночасно. Щоб продовжувати користуватися послугою, клієнт повинен здійснювати регулярні платежі, пролонгуючи термін дії послуги. Це можуть бути автоматичні платежі. В цьому випадку клієнт повинен залишити реквізити свого платіжного інструменту: номер картки або інше. Якщо ж ініціатором платежів буде клієнт, то в такому випадку за їх регулярністю повинен стежити сам клієнт. Це дуже важливий момент, який далі буде детально розглянутий. Клієнт на сайті білінгу бачить поточний стан, список своїх платежів (транзакцій). Клієнт може вибрати інший тарифний план. Клієнт може в будь-який момент відмовитися від послуги (cancel). Це означає, що послуга більше не буде пролонгуватись. Адміністрація білінгу формує тарифні плани, здійснює підтримку клієнтів, веде фінансову звітність.

Розглянемо білінг з точки зору кібербезпеки. Об’єктами кібернападу є відкриті сервіси: вебсервер, СУБД, або ж безпосередньо комп'ютери персоналу.

Розглянемо кібератаки на доступні з Internet сервера. Кібератаку можуть здійснювати: боти, людина, клієнт білінгу, оператор або адміністратор білінгу. Оператор або адміністратор білінгу не завжди можуть скоювати злочинні дії умисно. Їх облікові дані можуть бути вкрадені.

Таблиця 1

Складові кібератаки

Ціль атаки	Шлях реалізації
Неправомірне використання послуги білінгу	Крадіжка облікових даних клієнта Створення фейкових клієнтів Підміна умов тарифних планів Неправдива (помилкова) пролонгація послуги
Крадіжка грошей клієнта	Крадіжка платіжних реквізитів клієнта
Компрометація клієнта або білінгу	Крадіжка персональних даних клієнта
Крадіжка грошових засобів білінгу	Крадіжка або підміна платіжних реквізитів білінгу

Отже, з точки зору розподілу зон відповідальності кібербезпеки білінгу:

- Тарифні плани, фінансова звітність, реквізити прийому платежу – всі ці дані мають захищати система безпеки білінгу.
- Персональні дані клієнта потрібно зберігати в мінімальному обсязі.
- Список транзакцій та облікові дані клієнта для доступу до послуги повинен захищати білінг.

- Білінг повинен слідкувати за можливою компрометацією облікових даних клієнта.

Для захисту платіжних реквізитів клієнта їх краще винести за межі білінгу. Для цих цілей, як правило, використовуються провайдери платіжних послуг (Payment Service Provider, PSP). Наприклад: PayPal, CyberSource. Таким чином ще й підвищується ступінь довіри клієнта до білінгу. Білінг не зберігатиме у своїй базі даних (БД) платіжні реквізити клієнта, а буде зберігати тільки отриманий від PSP токен. Токен дозволяє здійснювати виключно тільки певні транзакції, що робить безглуздим його крадіжку. Шахрай не зможе за допомогою токена зробити платіж в свою користь. Крім того, клієнт отримує можливість відстежувати свої транзакції як на білінгу, так і на PSP.

Щоб відвідувач став клієнтом він повинен здійснити перший, стартовий платіж. Цей стартовий платіж може бути здійснений двома способами:

1. Дані клієнта приймає білінг на своєму сайті і далі його програмні модулі працюють з PSP API.

Переваги: робота з PSP прихована від клієнта; білінг негайно отримує повідомлення від PSP.

Недоліки: не дивлячись на те, що в БД білінг НЕ зберігає дані клієнта, є можливість втручання в канал передачі даних; злом програмних модулів білінгу надасть зловмиснику повні дані про клієнтів.

2. Білінг пересилає відвідувача на сайт PSP. Відвідувач виконує платіж на сайті PSP. Після чого білінг отримує повідомлення про платіж.

Недоліки: затримка через очікування повідомлення.

Як було зазначено вище, платежі можуть відбуватися автоматично або ж ініціатором платежів може бути клієнт. Деякі PSP підтримують автоматичні платежі. В цьому випадку білінг при створенні PSP-токена задає періодичність і суму платежів. Білінг повинен отримувати повідомлення від PSP в здійсненні подібних платежів. Якщо PSP не підтримує періодичних платежів, тоді білінг повинен сам періодично ініціювати платіж. Крім того, білінг повинен отримувати повідомлення про транзакції типу chargeback, які ініціюються PSP.

З точки зору розробника білінгу випадок, коли клієнт вирішує самостійно сплачувати користування послугою, можна розглядати як PSP, що підтримує автоматичні платежі. Білінг очікує отримання повідомлення про платіж. Відсутність повідомлення служить підставою в припиненні надання послуги.

У будь-якому випадку, необхідна система захисту каналу передачі таких оповіщень від втручання і прослуховування. А також необхідним є забезпечення гарантованої достовірної доставки повідомлення. Ці системи визначаються протоколами PSP.

Таким чином система забезпечення кіберзахисту білінгу повинна враховувати деякі вимоги:

- Застосовувати шифрування для забезпечення надійного та безпечного зберігання даних в базах даних.
- БД має бути зашифрована як на рівні файлів (тобто, засобами самої СУБД), так і на рівні застосунку. Тобто, сам білінг зашифровує дані перед збереженням їх в БД. Це шифрування ще й додатково ускладнює пошук даних. Резервні копії БД також повинні бути захищені шифруванням.
- Не зберігати платіжні реквізити клієнта в явному вигляді. Використовувати PSP токени.
- Персональні дані клієнта запитувати в мінімальному обсязі.
- Налаштування ключів шифрування, паролів, сертифікатів і тому подібного не повинно відбуватись в тому же вебінтерфейсі, що і робота служби підтримки та адміністрування, тому що взаємодія білінгу і PSP – одне з вузьких місць безпеки.

Наприклад, можна використовувати недоступну для запису вебсерверу файлову систему.

- Конфігураційні параметри зберігати в файлах. Вони доступні програмним модулям білінгу для читання. Вебсервер не має можливості зміни конфігурації.

В цьому випадку шахрай, зламавши вебсервер, не зможе підмінити дані.

- Доступ до сервісів білінгу з Internet має бути максимально обмежений. Наприклад, доступ до СУБД не відкривають.
- Доступ до каналів зв'язку білінг – PSP закритий для сторонніх клієнтів. Наприклад, через firewall.
- Постійний моніторинг за змістом ключів шифрування, сертифікатами та інше.
- Моніторинг здійснюється окремою незалежною системою з обов'язковим оповіщенням відповідальних осіб про всі факти зміни.
- Постійний аналіз БД. Контроль відповідності кількості клієнтів та їх транзакцій. Відповідність транзакцій на білінгу і PSP.