Безпечні комунікації без компромісів: Threema для корпоративного спілкування

Олексій ЗАЙОНЧКОВСЬКИЙ, керівник підрозділу інфраструктурних рішень в iIT Distribution, — про переваги корпоративного месенджера Threema.

Ніхто не може зазнавати безпідставного втручання у його особисте і сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або на його честь і репутацію.

*– **Загальна декларація прав людини**, стаття 12, 1948 р.*

Загальна декларація прав людини захищає право на приватність та пов'язані з нею персональні дані. Однак у сучасному світі Інтернету й соцмереж особиста інформація часто стає доступною іншим, адже зручність для користувачів нерідко переважає безпеку. Більшість платформ та систем комунікації користуються цим та використовують приватні дані для власних цілей або навіть як товар. Підтримувати високий рівень приватності чи забезпечувати анонімність у глобальній мережі не завжди доречно, але для корпоративного спілкування деприватизація даних становить значний ризик. На жаль, розгляд ризиків інформаційної безпеки часто обмежується захистом внутрішніх систем, тоді як конфіденційність користувачів та безпека їхніх комунікацій залишаються поза увагою.

Шахраї, фішинг та месенджери

Понад 80% користувачів передають робочу інформацію, зокрема конфіденційну, через месенджери. Відкритість соцмереж, де користувачі діляться детальними відомостями про своє життя, дозволяє зловмисникам легко створити точний портрет жертви і здобути її довіру, видаючи себе за «знайомого, якого важко пригадати». Месенджери надають прямий і швидкий доступ до користувача, оминаючи традиційні системи безпеки, що робить їх використання для обміну робочою інформацією небезпечним через ризик фішингу та розповсюдження шкідливого програмного забезпечення.

Монополії

Світ великих IT-компаній настільки монополізований, що держави й корпорації мають легкий доступ до даних користувачів, а деякі платформи відкрито заявляють про збір переписок і розмов. Лідирує в цій сфері холдинг Meta, маючи 2 мільярди користувачів у WhatsApp і 930 мільйонів у Facebook Messenger, що дозволяє йому безперешкодно диктувати політики конфіденційності.

У квітні 2024 року відбулося останнє велике оновлення умов конфіденційності та EULA (End User License Agreement), і користувачам дали всього кілька днів на прийняття нових умов або відмову від сервісу. Такий підхід виглядає як примусовий: коли всі особисті й робочі контакти зібрані в WhatsApp, відмовитися від нього майже неможливо — простіше натиснути «I Agree».

Масштабна база користувачів стає головною перевагою неспеціалізованих месенджерів, що природно приваблює користувачів для спілкування, але водночас створює серйозні ризики для безпеки та конфіденційності.

На що ми погоджуємось

Майже ніхто не читає всі умови сервісів та застосунків: це довго, складно сприймається і, зрештою, «А що ми можемо змінити?». Та все ж варто знати, на що ми погоджуємось.

IT-гіганти, як-от Apple, Meta та Google, є лідерами по збору персональних даних. Але одна справа збирати дати народження та адреси, і зовсім інша — безперервно стежити за користувачами.

Щоб краще зрозуміти масштаби проблеми, наведемо кілька прикладів з сайту аналітики збору приватних даних *https://justwhatsthedata.github.io/*.

Наприклад, **Telegram**, попри відому співпрацю з російським державним апаратом, залишається найбільш використовуваним месенджером в Україні. Telegram збирає:

• загальні дані користувача (ім'я, дата народження, e-mail, телефон);
• інформацію про пристрій (IP-адреса, браузер, тип пристрою);
• книгу контактів та календар;
• вміст усіх повідомлень, що означає повну відсутність приватності.

На виході маємо месенджер, який зберігає та аналізує абсолютно всі повідомлення, зокрема й секретні.

Інший приклад — **WhatsApp**. Окрім даних, які збирає Telegram, тут також відстежують:
• cookies;
• точне місцезнаходження;
• увесь завантажений контент;
• дані про з'єднання (Інтернет, Bluetooth);
• платіжні дані;
• Інформацію з інших застосунків (Facebook, Google, Apple);
• голосові дані з мікрофона;
• фото та відео з камери.

І це все подається за замовчуванням: або приймай — або видаляй.

Цікавим аспектом є наскрізне (End-to-End) шифрування, яким пишається месенджер. Насправді воно працює тільки для користувачів, тоді як для компанії — власника сервісу воно не діє. Це означає, що компанія або сторонні особи, за певних умов, можуть отримати доступ до оригінального вмісту розмов чи переписок, що суперечить концепції End-to-End шифрування.

Zoom та **Discord** також збирають чимало даних. Discord, який використовують геймери, підлітки і навіть волонтери, застосовує Google Analytics та додатково відстежує:
• поведінку в Інтернеті (Pixel tracking);
• спожитий контент (Web beacons);
• інформацію про браузер і його налаштування (Browser fingerprinting);
• дані про ОС мобільного пристрою (Device fingerprinting);
• встановлені застосунки.

Discord є лідером по збору персональних даних, і кілька років тому організацію навіть було оштрафовано на €800 тис. за порушення європейських законів про захист даних.

Задумайтесь, скільки інформації про вас накопичують і аналізують щодня. І хоча жарти «ми не дамо Вам дозвіл, бо 14 років тому Ви написали приятелю наступне...» можуть здаватися перебільшенням, реальність вже майже наздоганяє ці жарти.

Threema

Threema є піонером у сфері захищених комунікацій, де безпека (приватність і конфіденційність) ставиться вище за зручність. Цей корпоративний месенджер забезпечує гарантовано приватне або навіть анонімне спілкування. Основні переваги Threema для безпечних комунікацій такі.
• **Країна походження — Швейцарія:** нейтральна країна з позаблоковим статусом.
• **Справжнє End-to-End шифрування:** приватні ключі зберігаються лише на вашому пристрої, а сервери Threema діють лише як комутатори, не маючи доступу до даних.
• **Відсутність прив'язки до телефонних номерів чи електронної пошти:** конфіденційність користувачів на першому місці.
• **Жодних трекерів:** відсутність елементів, що відстежують активність.
• **Відкритий вихідний код:** можливість перевірки безпеки, що запобігає появі будь-яких прихованих елементів.
• **Комплексне on-prem встановлення:** повний контроль управління та безпеки.
• **Лише перевірені контакти в організації:** абсолютний захист від загроз фішингу.

Threema — це надійне рішення для тих, хто ставить безпеку комунікацій на перше місце.

Оптимальний варіант комунікацій: поєднання особистого та робочого

Оптимальний підхід до поєднання особистого і робочого спілкування — розділення середовищ. Якщо для спілкування з родиною, друзями та зовнішніми контактами доцільно використовувати загальнодоступні месенджери на власний розсуд і ризик, то для внутрішніх робочих комунікацій рекомендується використовувати Threema, де система може гарантувати «відповідність» кожного контакту конкретному пристрою, а також сталий закритий «периметр» організації, недоступний для неконтрольованих зовнішніх контактів. Особливо чутливу інформацію можна передавати через анонімні облікові записи, не пов'язані з конкретними особами; навіть адміністратори не знатимуть, хто є хто. Завдяки цьому вся конфіденційна інформація залишається в контрольованому середовищі та відповідає політикам безпеки.

Приватність — це законне право кожного громадянина сучасного світу, але цей світ побудовано там чином, що діють абсолютно протилежні «правила гри». Threema надає можливість створити власний «острів» безпеки та приватності та захистити робочі дані від зайвих очей.