Threema — запорука приватності комунікацій

Існує захищений месенджер, у якому всі комунікації здійснюються всередині корпоративної мережі і захищені від компрометації.

Фахівці з безпеки звикли до захисту типових каналів передачі інформації через глобальні та локальні мережі. Більшість компаній, які мають віддалених співробітників, також впровадили відповідні технології захисту доступу та даних, від VPN та мережевих екранів до ZTNA і DLP. Але не всі канали комунікацій захищаються однаково добре: зазвичай канали спілкування між співробітниками залишаються осторонь і взагалі не мають захисту.

За статистикою, більше ніж 80% співробітників використовують месенджери в робочих цілях. Таке спілкування пришвидшує комунікації та робить їх менш формальними, але при цьому, використовуючи загальнодоступні месенджери, ми нехтуємо безпекою та ставимо передачу конфіденційної або приватної інформації під загрозу. Більшість загальнодоступних месенджерів не має необхідного рівня захисту у вигляді end-to-end шифрування, а якщо і має, то централізована архітектура надає можливість компаніям-власникам розшифровувати дзвінки та повідомлення.

Популярні безпечні месенджери не такі безпечні, як хочуть здаватися

Нещодавно світові медіа писали про суперечку, яка виникла між деякими провідними світовими платформами обміну повідомленнями. 10 травня 2024 року президентка Signal Мередіт Віттакер виступила з критикою на адресу Telegram. У своєму дописі на платформі X (раніше Twitter) вона заявила:

«Telegram відомий своєю небезпечністю і регулярно співпрацює з урядами за лаштунками, попри свої великі заяви про свободу слова та конфіденційність. Навіть їхнє обмежене шифрування, яке треба самостійно налаштовувати, викликає підозри...».

Засновник Telegram Павєл Дуров стверджував, що повідомлення в Signal не такі приватні, як це подається, і заяви компанії про безпеку не можна перевірити. Проте це твердження рішуче спростовується Signal та широкою криптоспільнотою.

Деякі звинувачення здаються настільки надуманими, що більшість людей відразу відкидають їх як спробу підриву репутації конкурента. І хоча важливо залишатися скептичними стосовно неправдоподібних заяв, все ж варто пам'ятати, що насправді існує безліч випадків, коли нібито безпечні сервіси комунікації прослуховувалися або управлялися державними установами, чого користувачі не помічали.

Кожен, хто знайомий з безпечним зв'язком, повинен знати, що Telegram **не можна вважати безпечним за сучасними галузевими стандартами**. Це насамперед хмарний месенджер, з централізованою архітектурою, повідомлення постійно зберігаються на сервері без наскрізного шифрування, а тому можуть бути прочитані в будь-який момент. Увімкнути наскрізне шифрування можна лише в окремих чатах.

Натомість Signal відомий своєю криптографією (і був другим після Threema крос-платформним застосунком для обміну повідомленнями, що пропонує надійне наскрізне шифрування). Проте Дуров стверджує, що повідомлення Signal «важливих людей», з якими він спілкувався, були використані в американських судах або ЗМІ (ймовірно, маючи на увазі Такера Карлсона, який нещодавно взяв інтерв'ю у Дурова і раніше заявляв, що Агентство національної безпеки США зламало його акаунт у Signal).

Втім, подібні історії в Інтернеті можна знайти майже про будь-який захищений чат-застосунок. У тих випадках, коли це дійсно так, органи влади, швидше за все, змогли отримати фізичний доступ до мобільного пристрою, який міг належати одному з чат-партнерів підозрюваного. У резонансних випадках, звичайно, також можливо, що пристрій підслідного був заражений шпигунським програмним забезпеченням на рівні операційної системи. В такій ситуації скомпрометований весь пристрій, а безпека будь-якого застосунку, що працює на ньому, зникає.

Також хочеться нагадати про великий скандал в армії Німеччини після того, як

російські спецслужби отримали доступ до надсекретного запису розмови генералітету про ймовірне знищення мосту через Керченську протоку. Вони розмовляли через Cisco Webex та використали пароль для захисту сесії «1234». Це не жарт! Незрозуміло, чому німецький генералітет спілкується на такі теми через хмарний месенджер і чи взагалі він є обізнаним в сфері інформаційної безпеки, але є факт вилучення запису публічного хмарного сервісу.

Законодавчий аспект

У багатьох країнах на рівні законодавства хмарні провайдери послуг не мають права працювати, якщо їх сервери не розміщені на території країни, тож будь-який провайдер зобов'язаний надавати необхідну інформацію владі цих країн по запиту. Прикладами таких країн є США, Великобританія та інші країни НАТО, а також, звісно, росія. Отже, ми можемо легко дійти висновку, що месенджери, які досі працюють в рф, частково контролюються владою рф. Більшість провайдерів, звісно, скаже, що вони контролюють тільки свій сегмент користувачів, але жодних гарантій немає.

Централізована архітектура

Централізована архітектура месенджерів є типовою для публічного сегменту і, звісно, має переваги щодо зручності побудови та адміністрування, але разом з тим – великі вади з точки зору безпеки даних та приватності. Централізована архітектура надає можливість збирати та накопичувати дані про комунікації користувачів та контент, яким вони обмінюються. Зберігання всіх переписок та файлів на віддалених серверах є зручним для користувача, але це дає можливість читати всі повідомлення адміністраторам серверів. Такий сценарій може бути прийнятним для неформального спілкування з друзями, але зовсім не відповідає потребам спілкування з передачею конфіденційної інформації.

Окрім того, публічні месенджери можуть використовуватись для атак соціальної інженерії з метою подальшого отримання конфіденційної інформації або для інших зловмисних дій. Так само як і фішингові листи, в публічному месенджері ми можемо отримувати повідомлення від невідомих осіб, які можуть представлятися співробітниками або знайомими для входження в довіру та подальших маніпуляцій. Такі атаки зазвичай є добре спланованими, і перед їх здійсненням про жертву збирається вся інформація з соціальних мереж. На відміну від електронної пошти месенджер передбачає надання відповіді набагато швидше, що не залишає достатньо часу для осмислення ситуації.

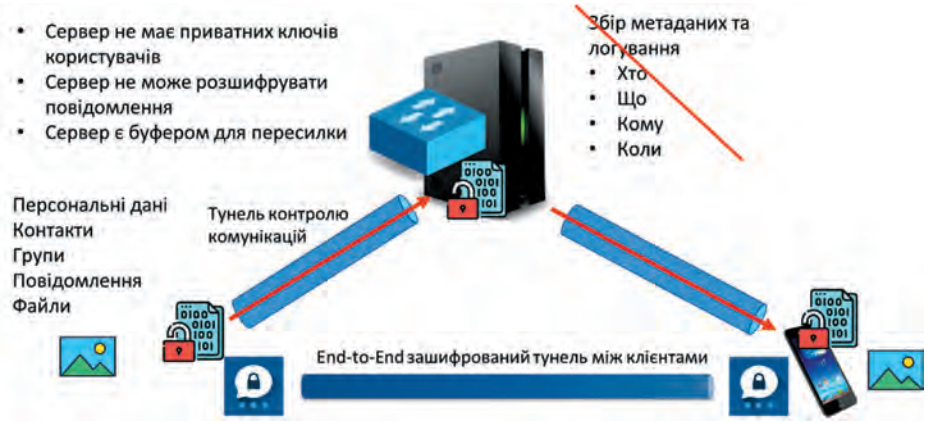

Рис. В Threema повідомлення не полишають корпоративної мережі

Всі описані вади безпеки та приватності можна легко вирішити, впровадивши корпоративний захищений месенджер, сервери якого будуть знаходитись у вас в інфраструктурі та не матимуть жодних зв'язків з сторонніми хмарними сервісами.

Рішення для бізнесу

Threema OnPrem — це сучасна платформа захищених комунікацій, яка розміщується на серверах замовника. Це забезпечує максимальну конфіденційність, оскільки всі дані зберігаються та обробляються всередині корпоративної мережі (**рис.**).

Threema є швейцарською компанією, а Швейцарія має позаблоковий нейтральний статус.

Сервери Threema не збирають інформацію про користувачів, технологія побудована таким чином, що сервер не може розшифрувати користувацький контент, а всі розмови та переписка шифруються напряму між клієнтськими пристроями (смартфонами, планшетами тощо). Сервери виступають тільки в ролі комутаторів, які зв'язують між собою пристрої.

Вся інформація повідомлень та файлів залишається на кінцевих пристроях.

Threema є єдиним месенджером, який дозволяє отримати абсолютну приватність комунікацій, для реєстрації користувача не потрібно надавати адресу електронної пошти, або номер телефону. Таким чином, Threema дозволяє створити абсолютно анонімний обліковий запис, з якого неможливо буде отримати персональні дані користувача. Це дає змогу створювати фактично анонімні комунікації, де тільки користувачі будуть знати, хто знаходиться на іншому пристрої, використовуючи довільні псевдоніми. Система ідентифікує користувача за Threema ID — це внутрішній ідентифікатор системи, який має наступний вигляд: YTND7ERX. Відповідно навіть адміністратори системи будуть бачити набір Threema ID, але не зможуть ні визначити, хто є власником, ані отримати доступ до переписки та дзвінків.

Threema — це сучасна платформа захищених комунікацій для співробітників, яка забезпечує максимальну конфіденційність та безпеку. Вона має замкнутий периметр, який не дозволяє стороннім особам отримувати доступ до даних, перевірений список контактів, індивідуальне шифрування всіх комунікацій та анонімність. Сьогодні Threema довіряють великі компанії, такі як Mercedes-Benz, силові структури та державні установи країн Євросоюзу.