УДК 004.6
DOI: 10.31733/17-03-2023-558-560

Андрій ДАНИЛОВ
старший викладач кафедри БІТ

Дарія ІВАЩЕНКО
студентка групи КБІКС-19-1 кафедри БІТ
Харківського національного університету
радіоелектроніки.

АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

В сучасному світі, де інформаційні технології є невід'ємною частиною нашого життя, захист інформації стає все більш важливим завданням. Незаконне вилучення інформації може призвести до серйозних наслідків, таких як порушення конфіденційності, цілісності та доступності даних.

З кожним роком збільшується кількість злочинів, пов'язаних з кібербезпекою. Зокрема, зловмисники застосовують різноманітні методи незаконного вилучення інформації, такі як фішинг, кібератаки, розповсюдження шкідливих програм тощо. Ці злочинні дії можуть призвести до значних фінансових втрат, порушення конфіденційності та приватності даних, а також вплинути на репутацію компаній та організацій.

Незаконне вилучення інформації є серйозною загрозою для конфіденційності, цілісності та доступності даних. Конфіденційні дані, такі як особисті дані або комерційна інформація, можуть бути викрадені і використані для злочинних цілей, таких як шахрайство, вимагання викупу або крадіжка особистої інформації. Цілісність даних також може бути порушена, якщо зловмисники вносять небажані зміни до даних або використовують методи шифрування для блокування доступу до даних власникам.

Крім того, доступність даних може бути обмежена, якщо зловмисники використовують методи Denial of Service або інші методи атак на мережу, щоб перевантажити систему і заблокувати доступ до даних. Таким чином, необхідні ефективні методи протидії незаконному вилученню інформації для збереження конфіденційності, цілісності та доступності даних.

Основні методи незаконного вилучення інформації можуть бути класифіковані за способом отримання даних. Основні методи незаконного вилучення інформації включають:

Фішинг − це метод, при якому злочинці використовують підроблені електронні листи або веб-сайти, щоб отримати доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, паспортні дані і т.д.

Віруси та троянські програми − це програми, які можуть використовуватись для вилучення конфіденційної інформації з комп'ютерів без дозволу власника. Віруси можуть поширюватись через електронну пошту, соціальні мережі або програми, які завантажуються з Інтернету.

Перехоплення трафіку − це метод, при якому злочинці перехоплюють трафік мережі, щоб отримати доступ до конфіденційної інформації, яку пересилають користувачі. Цей метод може бути використаний для отримання доступу до паролів, номерів кредитних карток та іншої конфіденційної інформації.

Фізичний доступ до даних − це метод, при якому злочинці отримують доступ до комп'ютерів або інших пристроїв, щоб викрасти конфіденційну інформацію. Цей метод може використовуватись в офісах або інших місцях, де зберігається конфіденційна інформація.

Соціальна інженерія − це метод, при якому злочинці використовують соціальні навички, щоб отримати доступ до конфіденційної інформації. Наприклад, злочинець може намагатись переконати працівника компанії надати йому доступ до системи, зробивши підробку ідентифікації або зламавши пароль. Також соціальна інженерія може включати в себе фішинг-атаки, коли злочинці надсилають електронні листи, які здаються легітимними, але насправді містять шкідливі посилання або додатки для вилучення інформації.

Існує кілька груп методів захисту від незаконного вилучення інформації, які допомагають зменшити ризики втрати даних і зберегти конфіденційність, цілісність і доступність інформації. Основні методи захисту інформації включають:

Фізичні методи захисту, такі як захист приміщення з обладнанням, забезпечення фізичної безпеки пристроїв зберігання даних, контроль доступу до приміщення з серверами і іншим обладнанням.

Організаційні методи захисту, які включають політики безпеки, культуру безпеки, процедури, правила і інструкції, що встановлюються в компанії для забезпечення безпеки інформації. Такі методи також включають регулярні навчання працівників з питань безпеки даних та аудит безпеки даних.

Технічні методи захисту, які включають захист мереж, захист даних, використання сильних паролів, шифрування даних, контроль доступу і ідентифікацію користувачів.

Юридичні методи захисту, такі як договірні зобов'язання, які обов'язковою умовою між компаніями, що мають доступ до конфіденційної інформації, і правові засоби, що захищають права на інтелектуальну власність та конфіденційність даних.

Технічні методи захисту від незаконного вилучення інформації включають в себе різноманітні технології, які допомагають захистити дані від несанкціонованого доступу. Одним з найбільш ефективних технічних методів захисту є шифрування даних. Шифрування забезпечує захист інформації шляхом перетворення її в код, який може бути прочитаний лише з допомогою ключа. Це ускладнює доступ до даних несанкціонованим особам, які не мають ключа до дешифрування.

Захист від вірусів та шкідливих програм також є важливим методом технічного захисту. Віруси та інші шкідливі програми можуть пошкодити або вкрасти дані, тому комп'ютери та інші пристрої повинні мати антивірусні програми та інші заходи захисту, такі як файрволи та антишпигунські програми.

Мережеві заходи захисту включають в себе використання мережевих протоколів та технологій, які дозволяють захистити мережу від несанкціонованого доступу. Мережеві заходи забезпечення інформаційної безпеки можуть включати в себе захист мережі від атак на віддалене виконання коду або захист від атак типу Denial of Service. Контроль доступу та ідентифікація є ще одним важливим методом технічного захисту. Цей метод включає в себе контроль доступу до систем та даних шляхом використання паролів, ідентифікаторів, карточок доступу та інших інструментів.

Крім того, існують технології, такі як біометричні системи, які дозволяють ідентифікувати користувачів за їхніми унікальними фізичними характеристиками, такими як відбиток, пальця форма обличчя тощо. Це дозволяє забезпечити більш точний та надійний контроль доступу до систем та даних. Інші технічні методи захисту включають встановлення брандмауерів та налагодження системи виявлення вторгнень, що дозволяють виявляти та запобігати спробам несанкціонованого доступу до системи. Також, методом захисту є резервне копіювання даних, яке дозволяє зберегти копію важливої інформації та відновити її у разі втрати.

Організаційні методи захисту також є важливою складовою системи захисту від незаконного вилучення інформації. Політики безпеки, культура безпеки та регулярні оновлення процедур допомагають забезпечити належний рівень захисту даних усередині організації. Політики безпеки визначають стратегії та процедури, яких необхідно дотримуватись для забезпечення безпеки даних, включаючи правила доступу до них, захист від вірусів та шкідливих програм, резервне копіювання даних та інші. Культура безпеки включає в себе свідомість персоналу щодо важливості захисту даних та навчання їх про правила безпеки та заходи, які слід вживати для їх захисту. Регулярне оновлення процедур та навчання персоналу допомагає забезпечити належний рівень захисту даних у всій організації.

Розглянемо декілька основних методів протидії незаконному вилученню інформації, серед яких:

Використання комплексної системи захисту: використання технічних, організаційних та юридичних методів захисту даних.

Регулярні оновлення програмного забезпечення: оновлення програмного забезпечення дозволяє закрити вразливості та запобігти злому.

Використання шифрування даних: шифрування даних дозволяє зберігати інформацію в зашифрованому вигляді, що ускладнює доступ до неї для зловмисників.

Політика безпеки та культура безпеки: розробка та впровадження політики безпеки, яка містить вимоги щодо захисту даних, а також створення культури безпеки серед співробітників.

Навчання персоналу: навчання співробітників технікам безпеки та правилам

користування комп'ютерною технікою та інформаційними системами.

Контроль доступу та ідентифікація: використання засобів контролю доступу до інформації та ідентифікації користувачів.

Резервне копіювання даних: регулярне створення резервних копій даних дозволяє відновити інформацію у разі її втрати або пошкодження.

Моніторинг та аудит безпеки: проведення моніторингу та аудиту безпеки даних для виявлення можливих загроз та слабких місць у системі інформаційної безпеки.

Методи незаконного вилучення інформації можуть бути дуже різноманітними і складними, тому потрібно розробляти ефективні методи їх протидії. Для цього необхідно розуміти потенційні загрози та використовувати відповідні методи захисту даних, щоб забезпечити їх конфіденційність, цілісність та доступність. Також важливо постійно оновлювати методи протидії відповідно до нових загроз та викликів, які постійно змінюються.

УДК 004.6
DOI: 10.31733/17-03-2023-560-561

Андрій ДАНИЛОВ
старший викладач кафедри БІТ

Катерина КОМАРЕЦЬ
студентка групи КБІКС-19-2 кафедри БІТ
Харківського національного університету
радіоелектроніки

АНАЛІЗ МЕТОДІВ ЗАХИСТУ КРИПТОВАЛЮТИ ВІД ЗЛОВМИСНИКІВ

Впродовж останніх років популярність криптовалюти постійно збільшується. Зі збільшенням попиту на використання криптовалюти збільшується кількість злочинів пов'язаних з криптовалютою. Саме тому, важливо захистити ці цифрові активи від зловмисників. У роботі наводяться результати аналізу методів захисту криптовалюти від зловмисників, зосереджені на використанні шифрування, аутентифікації та інших заходів безпеки.

Під час аналізу предметної галузі було виявлено багато різних методів захисту криптовалюти від зловмисників. Одним з найпоширеніших методів є використання криптографічних протоколів, які забезпечують захист від перехоплення та підробки транзакцій. Також існують методи захисту, що ґрунтуються на використанні технологій блокчейн та "розумних контрактів". Однак, незважаючи на наявність таких методів захисту, зловмисники все ще знаходять способи, щоб отримати доступ до криптовалют.

Криптовалюта − це форма цифрових або віртуальних грошей, що базується на криптографічних принципах та технологіях, які забезпечують безпеку транзакцій та контроль над створенням нових одиниць валюти. Криптовалюти працюють на основі децентралізованої системи, яка дозволяє користувачам проводити транзакції без посередництва банків чи інших посередників [4].

Шифрування є ключовим компонентом захисту криптовалюти від зловмисників. Шифрування – це процес перетворення даних у нечитабельну форму, що ускладнює доступ до даних. Криптовалютні гаманці використовують шифрування для захисту закритих ключів, які використовуються для доступу до гаманця. Крім того, багато бірж використовують шифрування для захисту даних, які вони зберігають, і запобігання доступу зловмисників до конфіденційної інформації [5].

Автентифікація є ще одним важливим заходом безпеки, який використовується для захисту криптовалюти від зловмисників. Автентифікація − це процес перевірки особи користувача перед тим, як дозволити йому отримати доступ до системи. Це часто робиться за допомогою паролів, двофакторної автентифікації, біометричної автентифікації або інших методів. Автентифікація гарантує, що лише авторизовані користувачі можуть отримати доступ до системи, таким чином запобігаючи зловмисникам отримати доступ.

Для захисту криптовалюти від зловмисників також можна використовувати інші заходи безпеки. Холодне зберігання − це спосіб зберігання криптовалюти в автономному