Міжнародний гуманітарний університет
Кафедра Комп'ютерної інженерії та інноваційних технологій

Лебедєва О.Ю.

ПРОГРАМУВАННЯ ТА ЗАХИСТ PLAY-ТЕХНОЛОГІЙ

методичні рекомендації для самостійної роботи
за темою «Стандарти кібербезпеки та криптографічний захист»
для здобувачів другого (магістерського) рівня,
які навчаються за спеціальністю 125 – Кібербезпека та захист інформації

Одеса 2024

Затверджено Вченою Радою Міжнародного гуманітарного університету (протокол № 13 від 16.08.2024 р.).

Лебедєва О.Ю.

Програмування та захист play-технологій: методичні рекомендації для самостійної роботи за темою «Стандарти кібербезпеки та криптографічний захист» для здобувачів другого (магістерського) рівня, які навчаються за спеціальністю: 125 – Кібербезпека та захист інформації [Електронне видання] / О.Ю. Лебедєва, кафедра комп'ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. Одеса, 2024. – 16 с.

Методичні рекомендації для самостійної роботи за темою «Стандарти кібербезпеки та криптографічний захист» для курсу «Програмування та захист play-технологій» призначені для з'добувачів, що навчаються за другим (магістерським) рівнем за спеціальністю: 125 – Кібербезпека та захист інформації. Дисципліна «Програмування та захист play-технологій» надає здобувачам знання в галузі комп'ютерних ігор та захисту інформації. На основі загальних понять в програмуванні та об'єктно-орієнтованого підходу дисципліна розглядає процес створення 2D-ігор в середовищі Unity, написання скриптів для реалізації функціональності гри та захисту даних.

ЗМІСТ

Історія появи міжнародних стандартів

1. Стандарт «Помаранчева книга»
2. Гармонізовані критерії європейських країн
3. Німецький стандарт BSI
4. Стандарт COBIT

1. Стандарт «Помаранчева книга»

Стандарти інформаційної безпеки (СІБ), головним завданням яких є створення основи для взаємодії між виробниками, споживачами та експертами з кваліфікації продуктів інформаційних технологій. Кожна з цих груп має свої інтереси і свої погляди на проблему ІБ.

Починаючи з початку 80-х років, були створені десятки міжнародних і національних стандартів у галузі інформаційної безпеки, які в певній мірі доповнюють один одного.

Найбільш відомі стандарти за хронологією їх створення:

- Критерій оцінки надійності комп'ютерних систем «Помаранчева книга» (США);
- Гармонізовані критерії європейських країн;
- Рекомендації X.800;
- Німецький стандарт BSI;
- Британський стандарт BS 7799;
- Стандарт ISO 17799;
- Стандарт «Загальні критерії» ISO 15408;
- Стандарт COBIT.

Історично першим оцінним стандартом, що набув широкого поширення і надав величезний вплив на базу стандартизації ІБ у багатьох країнах, став стандарт Міністерства оборони США "Trusted Computer System Evaluation Criteria" – Критерії оцінки безпеки комп'ютерних систем, або "Помаранчева книга", (названа за кольором обкладинки (рисунок 3.1)), вперше опублікований 1983 р.

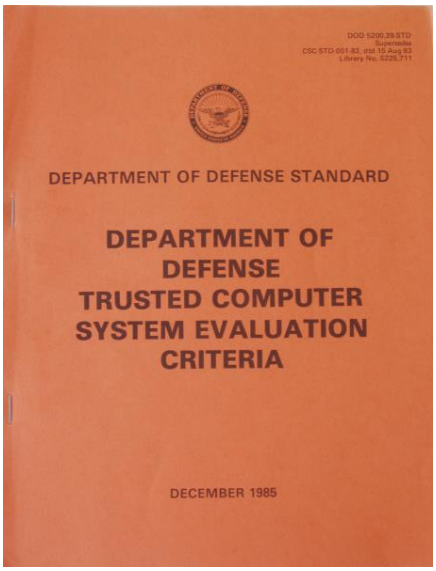

Рисунок 1 – Стандарт «Помаранчева книга»

«Помаранчева книга» пояснює поняття безпечної системи, яка «керує за допомогою відповідних засобів доступом до інформації так, що лише належним чином авторизовані особи або процеси, що діють від їхнього імені, отримують право читати, записувати, створювати та видаляти інформацію».

Вимоги «Помаранчевої книги» стали першою спробою створити єдиний стандарт безпеки КС, розрахований на проектувальників, розробників (програмістів), користувачів подібних систем та фахівців із їхньої сертифікації.

Згідно з «Помаранчевою книгою», політика безпеки повинна обов'язково включати в себе такі елементи:

- довільне керування доступом;
- безпека повторного використання об'єктів;
- мітки безпеки;
- примусове керування доступом.

Довільне управління доступом (дискреційним) – це метод розмежування доступу до об'єктів, заснований на обліку особистості суб'єкта або групи, в яку суб'єкт входить. Довільність управління полягає в тому, що деяка особа (зазвичай власник об'єкта) може на свій розсуд надавати іншим суб'єктам або відбирати у них права доступу до об’єкту.

Безпека повторного використання об'єктів – засіб управління доступом, що оберігає від випадкового або навмисного вилучення конфіденційної інформації зі «сміття». Безпека повторного використання повинна гарантуватися для областей оперативної пам'яті, для дискових блоків і магнітних носіїв в цілому.

Для реалізації примусового управління доступом з суб'єктами та об'єктами асоціюються мітки безпеки.

Мітка суб'єкта визначає його благонадійність, мітка об'єкта – ступінь конфіденційності інформації, що міститься в ньому.

Примусове (або мандатне) управління доступом базується на зіставленні позначок безпеки суб'єкта та об'єкта.

Суб'єкт може читати інформацію з об'єкта, якщо рівень таємності суб'єкта не нижчий, ніж у об'єкта, а всі категорії, перелічені в мітці безпеки об'єкта, присутні в мітці суб'єкта. У такому разі кажуть, що мітка суб'єкта домінує над міткою об'єкта.

Суб'єкт може записувати інформацію в об'єкт, якщо метка безпеки об'єкта домінує над міткою суб'єкта. Зокрема, «конфіденційний» суб'єкт може записувати дані до секретних файлів, але не може – у несекретні.

Мета підзвітності – у кожен момент часу знати, хто працює в системі і що робить.

Засоби підзвітності поділяються на три категорії:

- ідентифікація і автентифікація;
- надання довіреного шляху;
- аналіз реєстраційної інформації.

Звичайний спосіб ідентифікації – введення імені користувача при вході в систему. Стандартний засіб перевірки автентифікації користувача – пароль.

Мета надання довіреного шляху – дати користувачеві можливість переконатися в справжності системи, що обслуговує його.

Аналіз реєстраційної інформації (аудит) має справу з діями (подіями), що так чи інакше зачіпають безпеку системи. «Помаранчева книга» передбачає наявність засобів вибіркового протоколювання, як щодо користувачів (уважно стежити лише за підозрілими), так і щодо подій.

Абсолютно безпечних систем немає. Є сенс оцінювати лише ступінь довіри, яку можна надати тій чи іншій системі.

В «Помаранчевій книзі» довірена система визначається як «система, яка використовує достатні апаратні та програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу».

Помаранчева книга Міністерства оборони США відкрила шлях до ранжирування інформаційних систем за ступенем довіри безпеки. Було введено сім класів захищеності КС – від мінімального захисту (клас D1) до верифікованого (формально доведеного) захисту (клас A1).

Рівень D призначений для систем, визнаних незадовільними. У міру переходу від рівня C до A до систем висуваються дедалі жорсткіші вимоги. Рівні C і B поділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Класифікація:

- Рівень D. Мінімальний захист. До цього класу належать усі системи, які задовольняють вимогам інших класів.
- Рівень C. Дискреційний захист. Характеризується наявністю довільного управління доступом та реєстрацією дій суб'єктів.
- Рівень B. Мандатний захист. Основними вимогами цієї групи є нормативне управління доступом з використанням міток безпеки, підтримка моделі та політики безпеки, а також наявність специфікацій на функції ядра безпеки. Для систем цієї групи монітор взаємодій має контролювати всі події у системі.
- Рівень A. Верифікований захист. Характеризується застосуванням формальних методів верифікації коректності роботи механізмів керування доступом. Потрібна додаткова документація, яка демонструє, що архітектура та реалізація ядра безпеки відповідають вимогам безпеки.

Значення «Помаранчевої книги» важко переоцінити – це була перша спроба створення єдиного стандарту безпеки, і це був справжній прорив у галузі безпеки інформаційних технологій. Цей документ став точкою відліку для подальших досліджень і розробок. Основною його відмінністю є орієнтація на системи військового застосування.

2. Гармонізовані критерії європейських країн

Слідуючи по шляху інтеграції, європейські країни прийняли погоджені критерії оцінки безпеки інформаційних технологій (Information Technology Security Evaluation Criteria, ITSEC), опубліковані в червні 1991 року від імені відповідних органів чотирьох країн – Франції, Німеччини, Нідерландів і Великобританії.

Вигода від використання узгоджених критеріїв очевидна для всіх - і для виробників, і для споживачів, і для самих органів сертифікації.

Європейські критерії включають такі основні складові інформаційної безпеки:

- конфіденційність, тобто захист від несанкціонованого отримання інформації;
- цілісність, тобто захист від несанкціонованого зміни інформації;
- доступність, тобто захист від несанкціонованого утримання інформації та ресурсів.

У критеріях проводиться різниця між системами і продуктами.

Система – це конкретна апаратно-програмна конфігурація, побудована з цілком певними цілями і функціонуюча у відомому оточенні.

Продукт – це апаратно-програмний "пакет", який можна купити і за своїм розсудом вбудувати в ту чи іншу систему.

Таким чином, з точки зору інформаційної безпеки, основна відмінність між системою і продуктом полягає в тому, що система має конкретне оточення, яке можна визначити і вивчити як завгодно детально, а продукт повинен бути розрахований на використання в різних умовах.

Загрози безпеці системи носять цілком конкретний і реальний характер.

Щодо погроз продукту можна лише будувати припущення. Розробник може специфікувати умови, придатні для функціонування продукту; справа покупця – забезпечити виконання цих умов.

Для систем і продуктів вводиться єдиний термін – об’єкт оцінки. У відповідних місцях робляться застереження, які вимоги ставляться винятково до систем, а які – тільки до продуктів.

Кожна система і / або продукт висуває свої вимоги до забезпечення конфіденційності, цілісності та доступності. Щоб задовольнити ці вимоги, необхідно надати відповідний набір функцій (сервісів) безпеки, таких як ідентифікація і автентифікація, керування доступом або відновлення після збоїв. Сервіси безпеки реалізуються за допомогою конкретних механізмів.

Щоб об'єкт оцінки можна було визнати надійним, необхідна певна ступінь впевненості в наборі функцій і механізмів безпеки. Ступінь впевненості в пропонованому стандарті називається гарантованість. Гарантованість може бути більшою чи меншою в залежності від ретельності проведення оцінки.

Гарантованість зачіпає два аспекти – ефективність та коректність засобів безпеки. При перевірці ефективності аналізується відповідність між цілями, сформульованими для об'єкта оцінки, і наявним набором функцій безпеки. Крім того, в поняття ефективності входить здатність механізмів захисту протистояти прямим атакам (потужність механізму).

Визначаються три градації потужності – базова, середня і висока.

- Базовий – здатність протистояти окремим випадковим атакам;
- Середній – здатність протистояти зловмисникам з обмеженими ресурсами і можливостями;
- Високий – механізм може бути переможений тільки зловмисником високої кваліфікації з набором можливостей і ресурсів, що виходять за межі практичності.

У критеріях вводять термін – коректність, під якою розуміється правильність реалізації функцій і механізмів безпеки. Використовується сім можливих рівнів гарантованості коректності – від E0 до E6 (у порядку зростання). Рівень E0 позначає гарантована відсутність (аналог рівня D «Помаранчевої книги»).

При перевірці коректності аналізується весь життєвий цикл об'єкта оцінки – від проектування до експлуатації і супроводу. Загальна оцінка системи складається з мінімальної потужності механізмів безпеки і рівня гарантованості коректності.

Специфікації функцій безпеки - найважливіша частина опису об'єкта оцінки.

Критерії рекомендують виділити в цих специфікаціях розділи з наступними заголовками:

- Ідентифікація та автентифікація;
- Управління доступом;
- Точність інформації;
- Надійність обслуговування;
- Обмін даними.

Під ідентифікацією та аутентифікацією розуміється не тільки перевірка справжності користувачів у вузькому сенсі, але і функції для реєстрації нових користувачів і видалення старих, а також функції для генерації, зміни та перевірки аутентифікаційної інформації, в тому числі засоби контролю цілісності. Сюди ж відносяться функції для обмеження числа повторних спроб аутентифікації.

Засоби управління доступом також трактуються європейськими критеріями досить широко. У цей розділ потрапляють, крім інших, функції, що забезпечують тимчасове обмеження доступу до спільно використовуваних об'єктів з метою підтримки цілісності цих об'єктів – міра, типова для систем управління базами даних.

У цей же розділ потрапляють функції для управління розповсюдженням прав доступу і для контролю за отриманням інформації шляхом логічного висновку та агрегування даних.

Під точністю в критеріях розуміється підтримання певного відповідності між різними частинами даних (точність зв'язків) та забезпечення незмінності даних при передачі між процесами (точність комунікацій). Точність виступає як один з аспектів цілісності інформації.

Функції надійності обслуговування повинні гарантувати, що дії, критичні за часом, будуть виконані рівно тоді, коли потрібно – не раніше і не пізніше, та що некритичні дії не

можна перевести в розряд критичних. Повинна бути гарантія, що авторизовані користувачі за розумний час отримають запитувані ресурси.

Сюди ж відносяться функції для виявлення і нейтралізації помилок, необхідні для мінімізації простоїв, а також функції планування, що дозволяють гарантувати час реакції на зовнішні події.

До області обміну даними відносяться функції, що забезпечують комунікаційну безпеку, тобто безпеку даних, переданих по каналах зв'язку.

3. Німецький стандарт BSI

У 1998 році в Німеччині вийшло «Керівництво щодо захисту інформаційних технологій для базового рівня». Керівництво являє собою гіпертекст обсягом близько 4 МБ (у форматі HTML). Надалі воно було оформлено у вигляді німецького стандарту BSI.

Всі види загроз в стандарті BSI розділені на наступні класи:

- Форс-мажорні обставини;
- Недоліки організаційних заходів;
- Помилки людини;
- Технічні несправності;
- Умисні дії.

Аналогічно класифіковані контрзаходи:

- Поліпшення інфраструктури;
- Адміністративні контрзаходи;
- Процедурні контрзаходи;
- Програмно-технічні контрзаходи;
- Зменшення вразливості комунікацій; планування дій у надзвичайних ситуаціях.

Всі компоненти розглядаються і описуються за таким планом:

- загальний опис;
- можливі сценарії загроз безпеки (перераховуються застосовні до даної компоненті загрози з каталогу загроз безпеки);
- можливі контрзаходи (перераховуються застосовні до даної компоненті загрози з каталогу загроз безпеки);

4. Стандарт COBIT

Аудит інформаційної безпеки являє собою незалежну експертизу окремих областей функціонування організації. Розрізняють зовнішній і внутрішній аудит.

Зовнішній аудит – це, як правило, разове захід, що проводиться за ініціативою керівництва організації або акціонерів. Рекомендується проводити зовнішній аудит регулярно, а для багатьох фінансових організацій і акціонерних товариств це є обов'язковою вимогою з боку їх засновників та акціонерів.

Внутрішній аудит являє собою безперервну діяльність, яка здійснюється на підставі «Положення про внутрішній аудит» та у відповідності з планом, підготовка якого здійснюється підрозділами служби безпеки та затверджується керівництвом організації.

Питаннями аудиту інформаційної безпеки в даний час займаються різні аудиторні компанії, фірми організації, багато з яких входять до складу державних і недержавних асоціацій. Найбільш відомою міжнародною організацією займається аудитом інформаційних систем є ISACA, з ініціативи якої була розроблена концепція з управління інформаційними технологіями відповідно до вимог ІБ.

На основі цієї концепції описуються елементи інформаційної технології, даються рекомендації по організації управління і забезпечення режиму інформаційної безпеки.

Концепція викладена в документі під назвою COBIT 3rd Edition (Control Objectives for Information and Related Technology – Контрольні об'єкти інформаційної технології), який складається з чотирьох частин:

- частина 1 – короткий опис концепції (Executive Summary);
- частина 2 – визначення та основні поняття (Framework). Крім вимог і основних понять, в цій частині сформульовані вимоги до них;
- частина 3 – специфікації керуючих процесів і можливий інструментарій (Control Objectives);
- частина 4 – рекомендації щодо виконання аудиту комп'ютерних інформаційних систем (Audit Guidelines).

Третя частина цього документа в певному сенсі аналогічна міжнародному стандарту BS 7799. Приблизно так само докладно наведені практичні рекомендації з управління інформаційною безпекою, але моделі систем управління в порівнюваних стандартах сильно розрізняються.

Стандарт COBIT – пакет відкритих документів, перше видання якого було опубліковано в 1996 році. COBIT описує універсальну модель управління інформаційною технологією, представлену на рисунку 4.1.

Коротко основна ідея стандарту COBIT виражається наступним чином: всі ресурси інформаційної системи повинні управлятися набором природно згрупованих процесів для забезпечення компанії необхідної і надійною інформацією. У моделі COBIT присутні ресурси інформаційних технологій (IT), які є джерелом інформації, яка використовується в бізнес-процесі. Інформаційна технологія повинна задовольняти вимогам бізнес-процесу. Ці вимоги згруповані таким чином.

По-перше, вимоги до якості технології складають показники якості і вартості обробки інформації, характеристики її доставки одержувачу. Показники якості докладно описують можливі негативні аспекти, які в узагальненому вигляді входять в поняття цілісності та доступності. Крім того, в цю групу включаються показники, що відносяться до суб'єктивних аспектів обробки інформації, наприклад стиль, зручність інтерфейсів. Характеристики доставки інформації одержувачу – показники, в узагальненому вигляді входять в показники доступності і частково – конфіденційності і цілісності.

Розглянута система показників, по-перше, використовується при управлінні ризиками та оцінці ефективності інформаційної технології, по-друге, довіра до технології – група показників, що описують відповідність комп'ютерної інформаційної системи прийнятим стандартам і вимогам, достовірність оброблюваної в системі інформації, її дієвість. По-третє, показники інформаційної безпеки – конфіденційність, цілісність та доступність оброблюваної в системі інформації.

У стандарті COBIT виділені наступні етапи проведення аудиту.

Підписання договірної та початково-дозвільної документації. На цьому етапі визначаються відповідальні особи з боку замовника та аудиторської компанії, встановлюються рамки проведення аудиту, вказуються контрольовані елементи інформаційної системи, складається і узгоджується необхідна документація. За результатами попереднього аудиту всієї інформаційної системи проводиться поглиблена перевірка підозрілих з точки зору проведених аудитом компонентів системи.

Збір інформації із застосуванням стандарту COBIT, який в даному випадку регламентує склад об'єктів контролю досліджуваної системи. Ступінь деталізації опису об'єктів контролю визначається на етапі розробки вихідної дозвільної документації. При цьому намагаються домогтися оптимального співвідношення між тимчасовими, вартісними та іншими витратами на отримання вихідних даних та їх важливістю для цілей дослідження. Діапазон представлення вихідних даних змінюється від бінарних відповідей типу ТАК / НІ до розгорнутих звітів. Основна вимога до інформації, – це її корисність, тобто інформація повинна бути зрозумілою, доречною (відноситься до справи) і достовірної (надійної).

Аналіз вихідних даних проводиться тільки з урахуванням достовірних вихідних даних. Вимоги до проведення аналізу визначаються на етапі збору вихідних даних. Стандарт COBIT рекомендує застосовувати описані в стандарті методики аналізу даних, але при необхідності допускається використання дозволених ISACA розробок інших членів асоціації. На етапі аналізу можливе повернення до етапу збору інформації для одержання відсутніх вихідних даних.

Вироблення рекомендацій. Отримані в результаті проведеного аналізу рекомендації після попереднього узгодження з замовником обов'язково повинні бути перевірені на здійсниміcть і актуальність з урахуванням ризиків впровадження. Стандарт COBIT рекомендує оформляти рекомендації звітом про поточний стан інформаційних систем, технічному завданні на внесення змін, звітом про проведений аудит. Результати проведення аудиту можна поділити на три умовні групи: організаційні, технічні та методологічні. Кожна з названих груп спрямована на поліпшення організаційного, технічного або методологічного забезпечення інформаційної системи.

До організаційної групи відносяться оцінки стратегічного планування, загального управління та інвестицій в інформаційну систему, рекомендації, що сприяють підвищенню конкурентоспроможності компанії, зниження витрат на обслуговування інформаційної системи, результати перевірки відповідності інформаційної системи вирішувати бізнес-завдання, зниження вартості експлуатації інформаційної системи, управління ризиками, проектами , виконуваними в рамках інформаційних систем і деякі інші.

Технічна група результатів дозволяє краще зрозуміти проблеми інформаційних систем і розробити шляхи їх вирішення з мінімальними витратами, оцінити технологічні рішення, реалізувати весь потенціал нових технологій, системно вирішити питання безпеки, здійснити професійний прогноз функціонування і необхідності модернізації інформаційних систем, підвищити ефективність функціонування інформаційної системи, визначити рівень обслуговування інформаційних систем.

Методологічні результати дозволяють надати апробовані підходи до стратегічного планування і прогнозування, оптимізації документообігу, підвищенню трудової дисципліни, навчання адміністраторів і користувачів інформаційних систем, отриманню своєчасної та об'єктивної інформації про поточний стан інформаційної системи компанії.

Контроль за виконанням рекомендацій увазі постійне відстеження аудиторською компанією виконання замовником рекомендацією.

Підписання звітних актів приймання роботи з планом-графіком проведення подальших перевірок, розробкою такої додаткової документації, як довгострокові і короткострокові плани розвитку ІС, план відновлення інформаційної системи в надзвичайних ситуаціях, порядок дій при порушенні захисту, концепція політики безпеки. Постійне проведення аудиту гарантує працездатність системи, тому створення плану-графіка проведення подальших перевірок є однією з умов проведення професійного аудиту.

Всього в стандарті COBIT виділяється 34 завдання верхнього рівня обробки інформації.

Крім традиційних властивостей інформації – конфіденційності, цілісності і доступності, – в моделі додатково використовуються ще 4 властивості – дієвість, ефективність, відповідність формальним вимогам і достовірність. Ці властивості не є незалежними, оскільки частково пов'язані з першими трьома. Але їх використання пояснюється міркуваннями зручності інтерпретації результатів.

Застосування стандарту COBIT можливо як для проведення аудиту ІС організації, так і для початкового проектування ІС. Звичайний варіант прямої і зворотної задач. Якщо в першому випадку – це відповідність поточного стану ІС кращій практиці аналогічних організацій і підприємств, то в іншому – спочатку вірний проект і, як наслідок, по закінченні проектування – ІС, яка прагне до ідеалу.

Основними перевагами COBIT перед іншими аналогічними стандартами є те, що він дозволяє використовувати будь розробки виробників апаратно-програмного забезпечення та аналізувати отримані дані, не змінюючи загальні підходи і власну структуру.

Захист облікових даних

1. Захист облікових даних
2. Хешування облікових даних
3. Шифрування із збереженням формату

1. Захист облікових даних

Поняття небезпечного пароля пов'язане не так з його довжиною та кількістю спеціальних символів, як із шаблонами, які в ньому можна виявити.

У криптографії існує таке поняття, як ентропія чи міра невизначеності. Нам потрібні паролі із високою ентропією.

Важко повірити, але паролі більшості користувачів не є унікальними. Найпростіший шлях при підборі пароля до додатку – знайти список найпоширеніших паролів та провести атаку за словником.

Захистить не стільки довгий пароль, скільки пароль, в якому немає закономірностей, поширених слів і фраз. На жаль, донести це до користувачів важко. Тому слід ускладнити процес завдання пароля, наклавши на нього низку вимог. Слід заборонити використання пароля дат народження, імен, прізвищ або частин адреси.

Існує програмне забезпечення для перевірення надійності вашого пароля (https://bitwarden.com/password-strength/ або https://www.passwordmonster.com/).

За останні роки значно збільшилась кількість новин про крадіжку особистої інформації людей, оскільки вони припустилися простих помилок при створенні паролю. Розглянемо рекомендації, щоб скласти надійний пароль.

1. Не використовуйте один пароль для різних сервісів.

Понад дві третини користувачів в інтернеті роблять це, але це значно сприяє витоку даних. Відповідно такі «ключі» залишаються небезпечними протягом багатьох років після витоку.

Уникаючи створення абсолютно нового пароля для кожного облікового запису, люди також схильні повторно використовувати паролі з невеликими варіаціями, як-от додаткове число чи символ. Але їх також легко вгадати хакерам, і вони не можуть конкурувати з програмним забезпеченням, призначеним для швидкого тестування ітерацій вашого пароля.

2. Створюйте надійні паролі не лише для важливих облікових записів із «високим ризиком».

Багато користувачів створюють унікальні паролі лише для облікових записів, які, на їхню думку, містять конфіденційну інформацію або можуть бути зламаними, наприклад для онлайн-банкінгу чи бізнес-додатків.

Але навіть базова інформація про користувача, яка зберігається в одноразових облікових записах, може містити дані, які шахраї використовують, щоб видати себе за законних користувачів. Ваша адреса електронної пошти чи номер телефону можуть бути цінними для зловмисників у поєднанні з інформацією, викраденою під час інших зломів.

3. Використовуйте менеджери паролів.

На додаток до багатофакторної автентифікації, менеджери паролів є важливими інструментами, які можуть посилити вдалий пароль. Ці менеджери можуть допомогти вам створити унікальні одноразові паролі та автоматично заповнити їх в облікових записах, до яких вони прив’язані. Навіть якщо ви випадково клацнете фішингове посилання, ваш менеджер паролів може розпізнати невідповідність і відмовитися від автоматичного заповнення.

4. Створюйте складні паролі, що не містять особисту інформацію.

Найкращі паролі не обов’язково складні, але їх важко вгадати. Коди, які забезпечують високий рівень безпеки, є особистими для вас і не містять легко зібраної інформації, такої як ваше ім’я та дата народження. Наприклад, основою для надійних паролів може бути текст улюбленої пісні або ваше замовлення в ресторані.

Створюйте паролі, які містять принаймні 12 символів, і уникайте використання особистої інформації, яку легко вгадати. Вони також повинні запам’ятовуватися вам і містити різноманітні символи.

5. Активуйте систему багатофакторної аутентифікації.

Навіть найскладніші паролі можуть бути зламані. Багатофакторна автентифікація створює додатковий рівень безпеки, вимагаючи перевірки на додаток до вашого імені користувача та пароля кожного разу, коли ви входите в систему.

Найчастіше це робиться за допомогою одноразових паролів, надісланих sms або електронною поштою. Це додатковий крок, але він того вартий і створює ще одну перешкоду для зловмисників.

6. Дотримуйтесь звичок з безпеки.

Легко подумати, що з вами не станеться кібератак. Але враховуючи, що витік даних та інші кіберзагрози несуть високий ризик викрадення особистих даних, фінансових втрат та інших серйозних наслідків, найкраще підготуватися до найгіршого сценарію. Поки ви є користувачем інтернету, ви завжди будете потенційною мішенню, а байдужі звички до паролів ще більше збільшують ваш рівень ризику.

2. Хешування облікових даних

Конфіденційні облікові дані не можна зберігати у вигляді звичайного тексту. Перед першим збереженням слід хешувати пароль. Цей нескладний процес дає величезні переваги щодо безпеки.

Перевага хешування – низька ймовірність колізій. Так називається ситуація, коли різні вхідні дані дають однакову хеш-функцію. Відповідно, не доведеться турбуватися про те, що хакери «вгадають» пароль.

Усі паролі мають бути хешовані. Крім того, алгоритм хешування слід оцінювати за його математичною цілісністю та масштабуванням. При хешуванні на сучасному обладнанні алгоритм має бути повільним, що знижує кількість припущень в секунду, які може зробити запущений хакером сценарій злому.

При зломі паролів алгоритми повільного хешування сильно ускладнюють роботу хакера, який обов'язково автоматизуватиме процес. Як тільки хакер знайде ідентичний хеш до пароля, той фактично зламаний. Надзвичайно повільні хеш-алгоритми, такі як BCrypt можуть розтягувати час такого пошуку на роки.

Функція хешування BCrypt одержала свою назву від двох розробок. Літера «B» взята з назви шифру з симетричним ключем Blowfish Cipher, який був розроблений Брюсом Шнайєром (Bruce Schneier) у 1993 році і застосовувався як універсальний алгоритм шифрування, що вільно розповсюджується. А "Crypt" – це функція хешування, яка за умовчанням постачається з Unix-системами.

Алгоритм BCrypt поєднує в собі особливості як Blowfish, так і Crypt, але його швидкість хешування сповільнюється більш швидкому устаткуванні. Таким чином, що потужніше обладнання, то складніше шифрування.

3. Шифрування із збереженням формату

Хакерів часто приваблюють бізнеси, тому що вони витягують велику кількість ідентифікаційної інформації за один раз, а потім продають ці конфіденційні дані на чорному ринку. Незахищену персональну інформацію можна використовувати не тільки для крадіжки особистих даних, а для шахрайства та атак соціальної інженерії.

В ідеалі, кожна організація шифрувала б конфіденційні дані, коли це можливо, розшифровуючи лише тоді, коли потрібен доступ до відкритих текстових даних. Проте

застарілі програми та системи можуть очікувати, що дані будуть у певному форматі та не зможуть обробляти чи зберігати інші типи даних без істотних змін.

Це особливо критично для організацій, які використовують застарілі системи, чиї кодові бази та моделі даних не можна змінити або надто обтяжливі та ризиковані для оновлення. Наприклад, база даних, яка зберігає конфіденційні дані про охорону здоров'я, яка була введена в дію майже 20 років тому і продовжує працювати. Більшість організацій схильні до ризиків, пов'язаних з реструктуризацією такої ключової виробничої системи.

Наприклад, якщо для стовпцю бази даних, у якому зберігаються номера кредитних карток (з максимальним обмеженням довжини 16 символів) застосувати популярний симетричний алгоритм (наприклад, AES-256-GCM), то отриманий зашифрований текст, безсумнівно, перевищить максимальну довжину, дозволену базою даних, що призведе до помилок в обробці даних.

Виникає питання, як зашифрувати дані без реструктуризації чи руйнування бази даних. Популярним варіантом є шифрування із збереженням формату (з англ. FPE - Format-preserving encryption).

Шифрування із збереженням формату (FPE) — це процес шифрування даних таким чином, щоб вихідні дані (зашифрований текст) залишалися в тому самому форматі, що й вхідні дані (відкритий текст). Значення «формату» різне. Зазвичай використовуються лише кінцеві набори символів; цифровий, буквений або буквено-цифровий» [2].

FPE дає змогу розгортати широко поширене шифрування без критичних наслідків для застарілих систем. Додаткам, яким не потрібен доступ до конфіденційних даних, надаються шифртексти FPE. Якщо програмі потрібен доступ до даних, у робочий процес можна вставити функцію дешифрування, щоб надати доступ до відкритого тексту.

Ось кілька прикладів як можна застосовувати FPE:

- для перевірки платіжних карток: у секторі роздрібної торгівлі та електронної комерції дані платіжної картки необхідно збирати та зберігати для здійснення платежів. Крім того, працівникам може знадобитися переглянути та перевірити останні чотири цифри інформації платіжної картки клієнта. FPE полегшує надання працівникам лише необхідної інформації, залишаючи інші дванадцять цифр захищеними;
- для застарілих баз даних: телекомунікаційна система може мати безліч застарілих систем, які потребують використання зашифрованих даних для безпеки. Однак організація може не мати можливості реструктуризувати свої бази даних для зберігання зашифрованих даних. З FPE структура баз даних може залишатися незмінною.

Наступним терміном для аналізу є псевдонімізація, що походить від слова псевдонім. Псевдонім у перекладі з грецької означає «фальшиве ім'я», і відомим прикладом є вигаданий персонаж Брюс Вейн, якого іноді називають Бетменом. Подібно до Брюса Вейна та Бетмена, псевдонімізація в ІТ-системах означає, що ви маскуєте зареєстрованих користувачів та їхні особисті дані.

GDPR – це уніфікований закон про захист даних, що забезпечує права на конфіденційність інформації та встановлює для організацій правила обробки персональних даних громадян або резидентів країн, що входять до ЄС. Ці правила діють як запобіжники неправомірного використання чутливої інформації суб'єктів даних. Цей закон був розроблений Європейським парламентом і Європейською радою та набув чинності 25 травня 2018 року, замінивши Директиву про захист даних 1995 року.

У GDPR псевдонімізація визначається як «обробка персональних даних таким чином, що дані більше не можуть бути пов'язані з певним суб'єктом даних без використання додаткової інформації». Таким чином відбувається обмін особистими даними з неідентифікуючими даними, і для відтворення вихідних даних потрібна додаткова інформація. Крім того, додаткову інформацію слід зберігати окремо.

Псевдонімізація робить таку інформацію, як персональні ідентифікаційні номери та особисті дані менш доступною для неавторизованих користувачів у відповідності до вимог GDPR.

Наприклад, за допомогою анонімізації дані очищуються щоб виявлення будь-якої інформації, яка може служити ідентифікатором суб'єкта даних було неможливим. Натомість, псевдонімізація не видаляє всю ідентифікаційну інформацію з даних, а лише зменшує зв'язок набору даних з оригінальною ідентичністю особи (наприклад, за допомогою схеми шифрування)

Агентство Європейського Союзу з кібербезпеки (ENISA) опублікувало звіт «Методи псевдонімізації та найкращі практики», спровокований проблемами впровадження псевдонімізації на практиці. Посібник обговорює критерії вибору належних методів псевдонімізації, таких як захист даних, масштабованість і відновлення. Посібник також відображає конкретні випадки використання різних ідентифікаторів, таких як IP-адреса або адреса електронної пошти.

Для псевдонімізації поля «ім'я» потрібно замінювати реальне ім'я користувача на інше ім'я, яке буде схожим на інше реальне ім'я. Щоб виконати поставлену задачу, необхідно створити словник з унікальними людськими (в межах словника) іменами, достатньо великий, щоб алгоритм випадково вибраного числа міг обрати ім'я за його порядковим номером для подальшої заміни справжнього імені користувача. Потім в окремий словник з ключами для імен буде записано реальне ім'я користувача (значення) і порядковий номер фейкового імені (ключ) для подальшого процесу де-псевдонімізації.

Такий же процес буде і для псевдонімізації поля «прізвище», де потрібно замінювати реальне прізвище користувача на інше прізвище, яке буде схожим на інше реальне. Для виконання цієї задачі, знову ж таки необхідно створити словник з унікальними людськими прізвищами (в межах словника), достатньо великий, щоб алгоритм випадково вибраного числа міг обрати прізвище за його порядковим номером для подальшої заміни справжнього прізвища користувача. Потім в окремий словник з ключами для прізвищ буде записано реальне прізвище користувача і порядковий номер фейкового прізвища для подальшого процесу де-псевдонімізації.

Щодо удосконаленого методу псевдонімізації для поля «email» адреси, то процес передбачає відокремлення домену (domain) адреси від частини юзернейму (local-part) користувача, тому що маскувати чи шифрувати домен email адреси частіше за все не є виправданим. Процес псевдонімізації email адреси буде спиратися на замасковані ім'я та прізвище, щоб у вихідному (замаскованому і зашифрованому) датасеті дані виглядали як справжні. Для цього візьмемо першу букву замаскованого імені і ціле замасковане прізвище та поєднаємо їх через крапку.

Рекомендована література

1. Trusted Computer System Evaluation Criteria ["Orange Book"] URL: https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/dod85.pdf
2. Information Technology Security Evaluation Criteria (ITSEC) URL: https://www.sogis.eu/documents/itsec/itsec-en.pdf
3. Pseudonymization according to the GDPR [definitions and examples] URL: https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr/

Інформаційні ресурси

4. Password Strength Testing Tool [Електронний ресурс] URL: https://bitwarden.com/password-strength/
5. How Secure is Your Password? [Електронний ресурс] URL: https://www.passwordmonster.com/
6. Online Bcrypt Hash Generator & Checker [Електронний ресурс] URL: https://bcrypt-generator.com/