УДК 004.421.056.53(043.2)

Гладка В.
Салієва О.В.

РОЗРОБКА АЛГОРИТМУ ВІДСЛІДКОВУВАННЯ НЕСАНКЦІОНОВАНИХ ДІЙ КОРИСТУВАЧІВ У КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто поняття та основні форми несанкціонованих дій, проаналізовано механізми їх запобігання. За для забезпечення безпеки корпоративної інформаційної системи розроблено загальний алгоритм відслідковування несанкціонованих дій користувачів.

Ключові слова: Захист, інформація, несанкціоновані дії, корпоративна інформаційна система, відслідковування

Abstract

This article examines the concept and main forms of unauthorized actions, analyzes the mechanisms of their prevention. In order to ensure the security of the corporate information system, a general algorithm for tracking unauthorized user actions has been developed.

Key words: Protection, information, unauthorized actions, corporate information system, tracking.

Вступ

Одним із найцінніших активів будь-якого підприємства є комерційна таємниця, яка включає конфіденційну і цінну інформацію для бізнесу. Ця інформація повинна бути доступна лише уповноваженим співробітникам підприємства або окремим підрозділам. Метою даної роботи є вирішення проблеми захисту корпоративної інформаційної системи створенням безпечного середовища для обміну інформацією.

Дослідження

Несанкціоновані дії – це дії або активності, які відбуваються без попередньої згоди, дозволу або авторизації відповідної особи чи організації. Це означає, що особа, яка здійснює несанкціоновані дії, порушує встановлені правила, норми або закони [1].

Несанкціоновані дії можуть мати різні форми, зокрема:

1. Несанкціонований доступ: незаконне отримання доступу до комп’ютерних систем, приватної інформації, електронних ресурсів або приміщень без відповідних дозволів.
2. Несанкціоноване використання: використання чого-небудь без дозволу або поза встановленими рамками, таке як незаконне копіювання авторських матеріалів або використання чужих ідентифікаційних даних.
3. Несанкціоноване збереження або поширення: незаконне збереження, копіювання або поширення конфіденційної інформації без відповідної згоди.
4. Несанкціоновані трансакції: здійснення фінансових операцій або переказів коштів без належних повноважень або дозволу.
5. Несанкціоноване вторгнення: використання комп'ютерних систем або мереж для несанкціонованого доступу, розповсюдження вірусів або вчинення інших шкідливих дій [1].

Вчинення несанкціонованих дій спостерігається в різноманітних сферах суспільного життя. Наприклад, в електронному середовищі – хакерські атаки, фішинг, крадіжка особистої інформації або використання зламаних акаунтів. У фінансовому секторі – незаконне зняття грошей, шахрайство або використання крадених кредитних карток. В бізнес-середовищі несанкціоновані дії можуть включати порушення конфіденційності, викрадення комерційної інформації або порушення авторських прав.

Розглянемо основні механізми запобігання несанкціонованим діям користувача:

1. Автентифікація та авторизація: використання механізмів автентифікації для перевірки заявленої ідентичності користувачів перед наданням доступу до системи.

2. Обмеження привілеїв: надання користувачам тільки необхідних привілеїв для отримання доступу до системи. Застосування принципу найменшого привілею, де кожен користувач отримує лише необхідні дозволи для виконання своїх обов'язків. Це допоможе запобігти несанкціонованій зміні даних або доступу до конфіденційної інформації.

3. Шифрування даних: використання шифрування для захисту конфіденційної інформації, яка передається через мережу або зберігається на серверах.

4. Оновлення програмного забезпечення: регулярне оновлення програмного забезпечення корпоративної інформаційної системи, включаючи патчі безпеки та виявлення й усунення вразливостей. Застосування найновіших версії програми, щоб уникнути використання вразливостей, які можуть бути відомі зловмисникам [2].

5. Навчання та свідомість користувачів: забезпечити навчання користувачів щодо політик безпеки і правил використання корпоративної інформаційної системи. Проведення навчальних семінарів, надання пояснень щодо можливих загроз та наслідків несанкціонованої діяльності.

6. Моніторинг та аудит: встановлення системи моніторингу та аудиту, яка дозволяє відстежувати дії користувачів в інформаційній системі для виявлення відхилень та можливих порушень. Регулярна перевірка журналів подій та виявлення потенційних несанкціонованих дій.

7. Захист від зовнішніх загроз: для запобігання несанкціонованого доступу ззовні використовують різноманітні захисні механізми, такі як брандмауери, системи виявлення вторгнень, системи захисту від вірусів та інші.

8. Регулярне оцінювання ризиків: виконання регулярного оцінювання ризиків і аудит безпеки для ідентифікації нових загроз та слабких місць у системі. Загальна ідея полягає в поєднанні технічних та організаційних заходів для запобігання несанкціонованим діям користувачів в корпоративній інформаційній системі. Технічні заходи включають захист мережі та серверів, шифрування даних, моніторинг та аудит активності користувачів. Організаційні заходи включають політики безпеки, навчання користувачів та контроль доступу [3].

Важливо розуміти, що запобігання несанкціонованим діям користувача – це постійний процес, який вимагає безперервного моніторингу, оновлення та вдосконалення. Регулярне оновлення програмного забезпечення, навчання користувачів щодо нових загроз та підвищення їх свідомості з питань інформаційної безпеки є критичними аспектами для ефективного запобігання несанкціонованим діям [4].

З метою вирішення проблеми захисту корпоративної інформаційної системи розробимо алгоритм відслідковування несанкціонованих дій користувача, який базується на наступних кроках:

1. Визначення реєстрації подій: розробляється система реєстрації подій, яка включає моніторинг активності користувача. Ця система збирає дані про дії користувача, такі як вхід до системи, доступ до конфіденційних даних, зміна налаштувань тощо.

2. Аналіз та виявлення відхилень: застосовуються алгоритми аналізу даних для виявлення відхилень у активності користувача, які можуть свідчити про несанкціоновані дії. Це можуть бути незвичні патерни активності, спроби незаконного доступу до конфіденційної інформації, зміни в правах доступу без належних повноважень та інші аномальні активності.

3. Сигнали та сповіщення: у разі виявлення підозрілих дій користувача генеруються сигнали та сповіщення, що дозволяють операторам безпеки реагувати невідкладно. Це можуть бути автоматичні повідомлення, електронні листи або спеціальні сигнали на моніторах безпеки.

4. Інтервенція та реагування: при виявленні несанкціонованих дій користувача, вживаються відповідні заходи безпеки, які можуть включати призупинення доступу користувача до системи, блокування облікового запису, сповіщення відділу безпеки для подальшого розслідування та прийняття відповідних заходів.

5. Аудит та аналіз результатів: після застосування алгоритму проводиться аудит та аналіз результатів відслідковування несанкціонованих дій користувача, що включає перевірку ефективності алгоритму, виявлення можливих недоліків та вдосконалення системи безпеки.

6. Оновлення та вдосконалення: алгоритм постійно оновлюється та вдосконалюється на основі нових загроз та вимог безпеки. Застосовуються оновлення програмного забезпечення, алгоритмічні покращення та розширення функціоналу для ефективного виявлення та запобігання несанкціонованим діям користувачів.

Загалом, забезпечення кібербезпеки є важливою складовою сучасного життя. Правильне використання технологій, обережність та свідоме ставлення до онлайн-безпеки допоможуть залишатись захищеним в цифровому світі.

Висновок

Алгоритм відслідковування несанкціонованих дій користувача у корпоративній інформаційній системі є важливим інструментом для забезпечення безпеки та захисту конфіденційної інформації. Поєднання технічних та організаційних заходів дозволяє ефективно виявляти та реагувати на небезпечні дії користувачів. Аналіз результатів та постійне вдосконалення алгоритму допомагають забезпечити високий рівень безпеки в корпоративній інформаційній системі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Wimpelmann C. Detecting and Responding to Unauthorized Access [Електронний ресурс] / Christian Wimpelmann. – 2021. – Режим доступу до ресурсу: https://www.code42.com/blog/detecting-and-responding-to-unauthorized-access/.
2. rown, C. Anomaly Detection Techniques for User Behavior Analysis in Corporate Networks / Brown, C, Williams, E., 2020. – 52 с.
3. Yagiz Kaymak. Tracking User Application Activity by using Machine Learning Techniques on Network Traffic [Електронний ресурс] / Yagiz Kaymak, Roberto Rojas-Cessa. – 2019. – Режим доступу до ресурсу: https://www.researchgate.net/publication/331953548_Tracking_User_Application_Activity_by_using_Machine_Learning_Techniques_on_Network_Traffic.
4. Cypress Data Defense. How to Protect Your Data from Unauthorized Access [Електронний ресурс] / Cypress Data Defense. – 2020. – Режим доступу до ресурсу: https://www.cypressdatadefense.com/blog/unauthorized-data-access/.

Гладка Вікторія – студентка групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: gladka.viktoria@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», старший викладач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Hladka Viktoriia – student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: gladka.viktoria@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com