УДК 004.056

Чорна К.С.
Лукічов В.В.

Засіб моніторингу користувацької активності. Розробка модуля побудови профілів користувачів

Вінницький національний технічний університет

Анотація

В даній роботі досліджуються методи створення профілів користувачів для подальшого моніторингу їх активності. Застосунок для уникнення інцидентів викрадення конфіденційної інформації, на основі яких можна вважати, що з пристрою було здійснено крадіжка, зараження або інші дії, які порушують цілісність, конфіденційність або доступність. Розроблено метод прийняття рішень, щодо нормальної або ненормальної активності користувачів.

Ключові слова*: кібербезпека, профіль користувача, моніторинг активності, аналіз*

Abstract

The study describes methods for creating user profiles to further monitor their activity. An application to avoid incidents of theft of confidential information that may indicate that the device has been stolen, infected, or otherwise compromised for integrity, confidentiality, or availability. A method of decision-making on normal or abnormal user activity has been developed.

Keywords: *cybersecurity, user profile, activity monitoring, analysis*

Вступ

Багато галузей діяльності сучасного суспільства залежать від правильного функціонування незліченної кількості програмних засобів. Тому тема моніторингу користувачів є дуже актуальною, бо працівники іноді прагнуть несанкціонованого доступу до конфіденційної інформації, заразити шкідливим програмним забезпеченням всю мережу, або порушити цілісність файлів. Тому важливо проводити моніторинг користувацької активності задля уникнення таких інцидентів, такі випадки не повинні залишатись не покараними. Одним із способів покращення роботи корпоративної мережі є розмежування користувачів на групи та надання їм відповідних прав за допомогою політики безпеки.

Результати досліджень

Програмні засоби для моніторингу користувачів це насамперед тип програмного забезпечення для безпеки та спостереження, встановленого в окремій системі або корпоративній мережі[1]. Такі програми роблять передавання важливої корпоративної інформації більш захищеним та надійним. Також запобігають викрадення конфіденційної інформації, порушення цілісності та доступності. Моніторингом користувацької активності може слугувати як окремий додаток, так і частина програмного забезпечення. Існують також антивірусні програмні забезпечення або пакети програмного забезпечення для захисту інформації, які також виконують таку ж роль. На сьогоднішній день, існує багато методів, які реалізовані для моніторингу та управління діями користувача[2]:

- відеозаписи сеансів;
- збір та аналіз логів;
- перевірка мережевих пакетів;
- реєстрація натискань клавіш;
- моніторинг ядра;
- захоплення файлу або скриншота.

Вся інформація, зібрана у процесі використання будь якого метода моніторингу користувацької активності, повинна розглядатись, виключно опираючись на політику безпека компанії та ролей користувача,

щоб з'ясувати чи присутня у тій чи інший ситуації ненормальна активність. Ненормальна активність уособлює в собі, багато дій, починаючи від відвідування особистих сайтів або покупок у робочий час, закінчуючи крадіжкою конфіденційних даних компанії, таких як інтелектуальна власність або фінансова інформація.

Програми моніторингу можуть обробляти велику кількість даних, але основною їх задачею є знаходження та фільтрування інформації, яка важлива для захисту даних. Такі програмні засоби дають змогу, дізнатись безліч важливої інформації, щодо дій користувачів, наприклад, чи завантажують користувачі конфіденційні дані в хмари, чи використовують незатверджені служби та додатки, чи приймають участь у яких-небудь інших діях, застосовуючи мережу або інші ресурси компанії. Програми моніторингу також допомагають гарантувати, те що співробітники не викрадуть конфіденційну інформацію, після того як покинуть вашу компанію. Основною метою моніторингу активності користувачів – є безпека, тобто забезпечення захисту конфіденційної інформації[3].

Важливою складовою вдалого моніторингу користувацької активності є побудова профілів користувачів, що дає змогу розмежувати користувачів на групи та надати їм відповідні права. Профіль користувача – це, по сутті, сукупність налаштувань та інформації, пов'язаних із користувачем[4]. Його можна визначити як чітке цифрове відображення особистості користувача в операційному середовищі, будь то операційна система, програмне забезпечення або веб-сайт.

Складовими частинами профілю кожного користувача є різні налаштування і всі ярлики, розміщені користувачем на робочому столі. Взагалі в профілі зберігаються всі призначені для користувача настройки Windows і додатків, з якими працює користувач. Зазвичай, у профілях користувачів є багато корисної інформації про велику кількість атрибутів, наприклад, системні потреби, загальні дані, обмеження та налаштування програм. Кожен профіль, будь-якого користувача можна створювати, змінювати та видаляти.

Моделювання користувачів є підрозділом взаємодії людини з комп'ютером, що описує процес побудови та модифікації концептуального розуміння користувача[5]. Системі потрібно внутрішнє представлення користувача для того, щоб адаптувати систему до конкретних потреб користувача. Ще однією метою вважають, моделювання навичок та декларативних знань для конкретних типів користувачів. Потрібно зібрати персональні дані, пов'язані з конкретним користувачем, щоб отримати модель користувача.

Модель користувача - це структура даних, яка використовується для фіксації певних характеристик окремого користувача, а профіль користувача є фактичним поданням у даній користувацькій моделі. Існують різні шаблони проектування для користувацьких моделей, інколи використовується їх суміш, представленні в таблиці 1[6].

Таблиця 1 – Шаблони проектування для користувацьких моделей.

Вид моделі користувачів	Короткий опис
Статична	Найосновніший тип моделі. Зібрані дані не змінюються. Вони статичні. Для зміни моделі не використовується алгоритм навчання
Динамічна	Моделі можуть бути оновлені та враховувати поточні цілі та потреби користувачів, за рахунок зміни в інтересах користувачів або взаємодії з системою.
На основі стереотипів	Користувачі класифікується на основі загальноприйнятих стереотипів. Такі моделі покладаються на статистику, ігноруючи особисті атрибути.
Високоадаптивна	Забезпечують високу адаптивність системи. Прагнуть знайти конкретне рішення для кожного користувача. Потребує збору інформації.

Перераховані вище види побудови моделі дають змогу розмежувати користувачів на відповідні групи, після чого надати їм відповідні права.

Висновки

Отже, запропонований модуль програмного засобу є системою прийняття рішень, яка допомагає аналізувати поведінку користувача на основі вхідних даних з модуля моніторингу користувацької активності та визначити чи активність профілю є нормальною чи аномальною.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке програмне забезпечення для моніторингу? Режим доступу: https://sales-generator.ru/blog/kontrol-raboty-sotrudnikov/.
2. What is user activity monitoring? How it works, benefits, best practices, and more. Режим доступу: https://digitalguardian.com/blog/what-user-activity-monitoring-how-it-works-benefits-best-practices-and-more
3. User activity monitoring and access logging tool. Режим доступу: https://www.solarwinds.com/security-event-manager/use-cases/user-activity-monitoring
4. Що таке профіль користувача? Режим доступу: https://uk.theastrologypage.com/user-profile#menu-1
5. Gerhard Fischer: A taxonomy of recommender Agents on the Internet Режим доступу: https://link.springer.com/article/10.1023/A:1011145532042
6. Miquel Montaner, Beatriz Lopez, Josep Liuis de Ll Rosa: A taxonomy of recommender Agents on the Internet Режим доступу: https://link.springer.com/article/10.1023/A:1022850703159

Чорна Катерина Сергіївна — студентка групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: kate.black.vin@gmail.com.

Лукічов Віталій Володимирович — кандидат технічних наук, старший викладач кафедри захисту інформації, Вінницький національний технічний університет , м. Вінниця, e-mail: lukichov.vitalyi@vntu.edu.ua.

Chorna Kateryna — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : kate.black.vin@gmail.com.

Vitaliy Lukichov – PhD (Eng), Senior Lecturer of Information Protection Department, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua.