РЕШЕНИЕ ПРОБЛЕМЫ УТЕЧКИ КОРПОРАТИВНЫХ ДАННЫХ С ПОМОЩЬЮ СИСТЕМЫ МОНИТОРИНГА АКТИВНОСТИ СОТРУДНИКА

Гончаренко Д.А.[1], Самойлов И.С.[3], Жуковский О.И.[2]
[1] Томский государственный университет систем управления и радиоэлектроники, АОИ, 421-М1, email: ice.post.yandex@gmail.com
[2] Томский государственный университет систем управления и радиоэлектроники, АОИ, к.т.н., доц. кафедры АОИ, email: oleg.i.zhukovskii@tusur.ru
[3] Томский политехнический университет, ИШИТР, 8В91, email: iss32@tpu.ru

Введение

Безопасность данных стала важнейшей проблемой в современном цифровом мире, поскольку несанкционированное раскрытие конфиденциальной информации может иметь очень серьезные последствия. Проблема утечки данных является сложной и требует комплексного подхода, сочетающего технические, организационные и человеческие элементы для обеспечения сохранности и безопасного доступа к информации. Существует множество различных подходов, которые компании могут применять для снижения риска утечки данных. В данной работе представлена реализации программного продукта (далее - ПП), который позволяет автоматизировать процесс сбора, обработки и хранения данных о производимых операциях при взаимодействии сотрудника с персональным компьютером (далее - ПК).

Анализ области

Утечки данных — это инциденты, при которых конфиденциальная информация раскрывается лицам, не имеющим права доступа к данной информации. Последствия могут варьироваться в зависимости от типа информации и того, какие возможности ее использование предоставляет злоумышленникам [1]. Попадание информации к злоумышленникам, или предоставление ее в публичный доступ, могут привести к потере репутации, юридическим издержкам, финансовым потерям и раскрытию личной информации.

Согласно полученным данным от федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее - РКН), за 2022 год произошло около 150 крупных утечек [2]. Только за январь 2023 года произошло несколько крупных утечек, таких как утечка персональных данных у компаний 1С, Mail.Ru Group, Спортмастер. Был опубликован исходный код различных сервисов у Яндекс в размере 44,7 Гбайт [3]. По статистике, в большинстве случаев утечка информации происходит по вине самих сотрудников организации. На рисунке 1 продемонстрирована мировая статистика по виновникам в утечке информации [4].

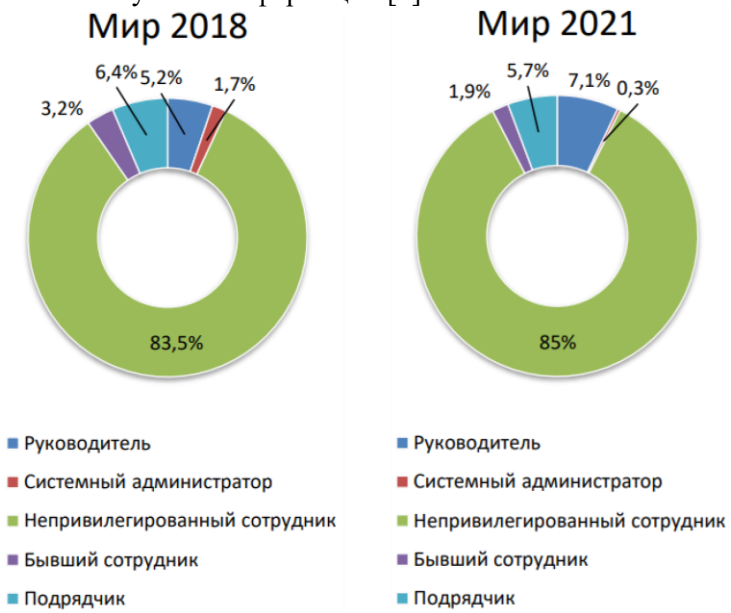


Рис. 1. Статистика в процентном соотношении по виновникам в утечки информации

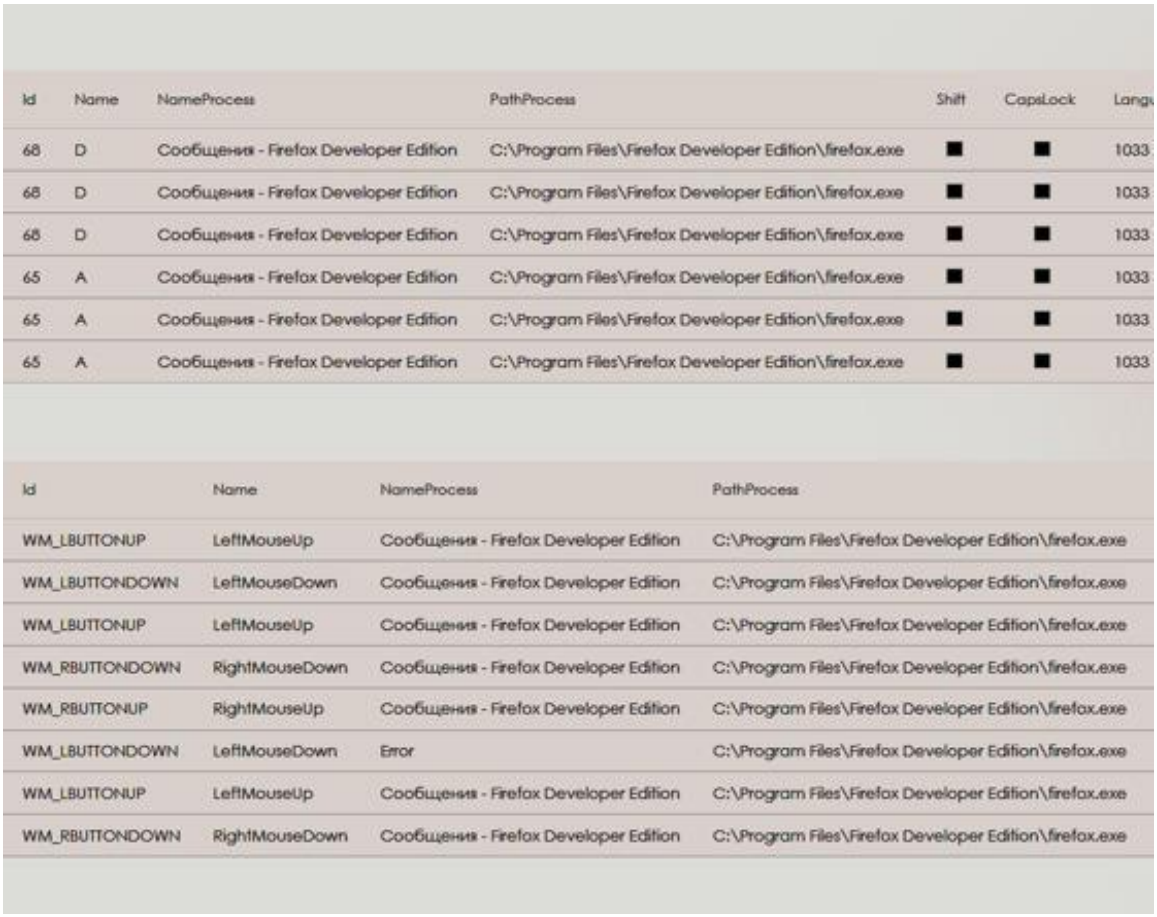
Основываясь на имеющейся статистике, можно сделать вывод, что большая часть утечки информации приходится на руководителя и сотрудников компании и данный показатель за три года вырос. Данный тренд означает необходимость средств мониторинга сотрудников для обеспечения безопасности данных.

Проблема утечек данных в организационной среде требует программных решений. Перед началом разработки ПП был определен подход и проанализирован функционал в уже существующих средствах мониторинга. Анализ на основе более десяти решений показал, что основная масса решений работает только на операционной системе (далее - ОС) Windows. В качестве подхода используется подписка на хуки (Hook) на основе Win32 API. Когда в системе происходит событие, то информацию об этом получает программа. В качестве функционала в большинстве случаев был выделен мониторинг, логирование, скриншоты экрана, запись микрофона и генерация отчётов. Из всех рассмотренных решений, только одно решение было от отечественной компании.

Разработка

На основе анализа были выявлены основные требования к функционалу нового ПП, которые использовались в данной разработке. Основой функционала является поддержка операционных систем Windows, Linux и macOS, генерация отчётов и выгрузка данных в различных форматах, получение данных в режиме реального времени, шифрование, обработка сочетаний клавиш и получение сообщений о несанкционированном доступе.

Основой реализации являются языки программирования C++ в связке CMake и JavaScript на платформе Node.js, а в качестве СУБД используется MongoDB. Получение статистики и отчетов, как сотрудник взаимодействует с ПК в течение определенного периода, реализовано в приложении настольной и веб-версии. На рисунке 2 показан графический интерфейс веб-версии.



Id	Name	NameProcess	PathProcess	Shift	CapsLock	Langu
68	D	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033
68	D	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033
68	D	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033
65	A	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033
65	A	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033
65	A	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe	■	■	1033

Id	Name	NameProcess	PathProcess
WM_LBUTTONUP	LeftMouseUp	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_LBUTTONDOWN	LeftMouseDown	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_LBUTTONUP	LeftMouseUp	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_RBUTTONDOWN	RightMouseDown	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_RBUTTONUP	RightMouseUp	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_LBUTTONDOWN	LeftMouseDown	Error	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_LBUTTONUP	LeftMouseUp	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe
WM_RBUTTONDOWN	RightMouseDown	Сообщения - Firefox Developer Edition	C:\Program Files\Firefox Developer Edition\firefox.exe

Рис. 2. Графический интерфейс веб-версии

Для работы с базой данных и генерации различных отчетов был реализован сервер, который обрабатывает запросы по протоколу связи WebSocket (далее - WS) и TCP. Получение данных о действиях

пользователя обеспечивает программа, работающая в фоновом режиме без графического интерфейса. В зависимости от ОС по-разному выполняется обработка событий, результаты которой далее передаются в функцию для отправки данных к серверу для сохранения в БД по WS. Реализована отправка сообщений на почту или в мессенджер Telegram. Система поддерживает получение экстренных оповещений с информацией о запуске сторонних программ, подключении неизвестных сторонних девайсов, запуске компьютера сотрудника, который отсутствует в данный момент и иных случаях потенциально несанкционированного доступа. Реализованный функционал по мониторингу в реальном времени позволяет оперативно и эффективно реагировать на возникающие проблемы корпоративной безопасности.

Заключение

Результатом данной работы является один из вариантов решения проблемы утечки корпоративных данных с помощью системы мониторинга сотрудников, основанное на технологии логирования действий сотрудника на конкретном ПК. Представленное в данной работе программное решение, реализованное в виде законченного ПП, позволяет снизить риск утечки информации т.к. система экстренного оповещения позволит службе безопасности компании реагировать гораздо быстрее. Также ПП позволит уменьшить сроки на расследование инцидентов в случае, если утечка информации всё-таки была совершена. Дополнительно стоит отметить, что данный продукт позволит произвести импортозамещение т.к. ранее было сказано, что аналоги данного продукта в основном являются зарубежными.

Список использованных источников

1. Что такое «утечка данных» и как предотвратить эту угрозу. [Электронный ресурс]. – URL: https://www.securitylab.ru/analytics/512440.php (дата обращения 09.02.2023).
2. Роскомнадзор об утечки данных. [Электронный ресурс]. – URL: https://vk.com/rkn?fixed=1&w=wall-76229642_258370 (дата обращения 09.02.2023).
3. Утечки данных в России. [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_России (дата обращения 09.02.2023).
4. Отчёт об утечках данных за 1 полугодие 2022 года. [Электронный ресурс]. – URL: infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения 09.02.2023).