DOI 10.37882/2223–2966.2022.08.25

ФИЛОСОФИЯ ИНФОРМАЦИОННОЙ ГИГИЕНЫ: НЕСКОЛЬКО ПРОСТЫХ СПОСОБОВ ЗАЩИТИТЬ ОРГАНИЗАЦИЮ ОТ УТЕЧКИ ДАННЫХ

THE PHILOSOPHY OF INFORMATION HYGIENE: A FEW SIMPLE WAYS TO PROTECT AN ORGANIZATION FROM DATA LEAKAGE

O. Laminina
R. Laminin

Summary. The article is devoted to alternative ways to prevent data leakage from the corporate infrastructure of organizations belonging to different verticals. As well as exfiltration of data from mobile devices of employees of these companies. The article considers the relevance and necessity of changing the view and approach to the modern philosophy of enterprise information protection. The paper considers the use of robotics tools of various processes, the use of web isolation tools, tools that make it difficult to profile employees, and, consequently, prevent attacks by means of social engineering. It also describes the need to create and conduct various educational events for employees.

Keywords: information security, cyberattack, authentication, phishing, malicious software, exfiltration.

Ламинина Ольга Глебовна
К.ф.н., доцент, Национальный исследовательский университет Московский государственный технический университет им. Н.Э. Баумана
olga.laminina@ngips.ru
Ламинин Роман Анатольевич
Аспирант, Национальный исследовательский университет Московский государственный технический университет им. Н.Э. Баумана
ral@ngips.ru

Аннотация. Статья посвящена альтернативным способам предотвращения утечки данных из корпоративной инфраструктуры организаций, принадлежащих различным вертикалям. А также эксфильтрации данных с мобильных устройств сотрудников этих компаний. В статье рассмотрена актуальность и необходимость изменения взгляда и подхода к современной философии защиты информации предприятий. Рассматривается применение средств роботизации различных проессов, применение средств вебизоляции, средств затрудняющих профилирование сотрудников, а, следовательно, предотвращающих атаки средствами социальной инженерии. Также описывается необходимость создания и проведения различных образовательных мероприятий для сотрудников.

Ключевые слова: информационная безопасность, кибератака, аутентификация, фишинг, вредоносное программное обеспечение, эксфильтрация.

Введение

Изначально, скорость хакерской атаки зависела исключительно от квалификации злоумышленника и, как ни странно, от скорости печати. Вчерашние ручные хакерские атаки сегодня полностью автоматизированы за счет использования вредоносного программного обеспечения.

Обычная организация подвергается более 300 кибератакам в день, при этом полноценное расследование всего одной из них занимает примерно от 30 минут до 8 часов. Ни в одна организация не может позволить себе такое количество персонала, чтобы провести тщательный анализ всех этих атак. Кроме того, атаки на основе вредоносного программного обеспечения могут начинаться и заканчиваться в течение менее 15 минут. При таких скоростях ни один автоматизированный ситуационный центр, не говоря о ручном анализе, не сможет предотвратить утечку данных.

Любая кибератака тщательно готовится, также как, например, ограбление банка в реальном мире. Злоумышленнику необходимо получить максимум информации о банке, сотрудниках, сигнализации, сейфе, кодах и т.д. В виртуальном мире тоже самое, и так же работают методы социальной инженерии. Традиционных средств защиты — межсетевых экранов, систем предотвращения вторжений, антивирусов, уже недостаточно. Следовательно, необходимо действовать на превентивном уровне.

Многие отрасли, находящиеся в зоне риска, в том числе финансовые организации, образование и частный бизнес, подсчитывают количество утечек больших объемов данных за минувший год. По данным Центра

по борьбе с хищениями личных данных, число утечек данных в мире в 2021 году взлетело на 82% [1].

Рекомендации по предотвращению утечки данных

Рассмотрим несколько недорогих способов усиления системы ИБ инфраструктуры большинства организаций. Каждый из этих способов не является панацеей, однако применение их в комплексе гарантированно повысит уровень безопасности предприятия.

Проблема:

В связи с пандемией вопрос по организации удаленной работы сотрудников вышел на передний план. В сложившейся ситуации уже не стоит вопрос о том, должен ли сотрудник работать из дома, сейчас это уже нормальная практика.

Самая большая проблема, с которой сталкиваются сотрудники отделов ИБ — это использование удаленно работающими сотрудниками своих устройств для выполнения должностных обязанностей, и соответственно, это утечка приватных данных с этих устройств.

Если мобильные устройства постоянно включены — это значит, что данные с них постоянно утекают, то есть происходит эксфильтрация данных.

Что такое эксфильтрация данных?

Эксфильтрация данных — это несанкционированное копирование, передача или извлечение данных с компьютера или сервера. Такая ситуация возникает, когда вредоносное ПО и/или злоумышленник осуществляет несанкционированную передачу данных с компьютера. Эксфильтрация данных также считается одной из форм кражи.

Процесс эксфильтрации очень трудно обнаружить, потому что он происходит на заднем плане, жертва даже не осознает, что что-то произошло, а утечка приватных данных делает уязвимыми не только отдельных пользователей, но и организации к атакам с помощью методов социальной инженерии. Сейчас кибератаки растут как в количественном, так и в качественном плане. Рано или поздно, вредоносное ПО будет установлено на устройство. Такие вредоносные программы часто остаются скрытыми и активируются только тогда, когда машина простаивает в течение определенного периода времени или по определенному системному событию. Люди часто удивляются, сколько данных передают и получают их мобильное устройство за ночь, когда они даже не пользовались своим смартфоном или планшетом.

Распространенные методы включают анонимизацию подключений к сторонним серверам для защиты личности злоумышленника. Например, использование DarkWeb, прямые IP-адреса, инкапсуляцию трафика в протоколы SSL/TLS и бесфайловые атаки, где злоумышленники могут использовать удаленное выполнение кода.

Решение:

Стандартных систем обнаружения вторжений, МЭ, антивирусов недостаточно для предотвращения утечки данных. В подобной ситуации используется технология реверсивного межсетевого экрана.

Реверсивный МЭ останавливает кибератаки в режиме реального времени, сосредоточившись на предотвращении утечки данных, профилировании хозяина устройства и сбора о нем приватных данных. Подобная технология защищает от современных угроз, заполняя пробел между решениями безопасности, фокусирующимися на предотвращении доступа с помощью систем охраны периметра (межсетевые экраны, IDS/IPS, антивирусы).

Реверсивный МЭ — это единственная технология, которая обеспечивает защиту от эксфильтрации данных с устройства и гарантирует, что никакие данные никогда не отправятся в публичную сеть, а также это единственное решение, способное блокировать исходящий поток данных. Множественные уровни защиты реверсивного МЭ защищают от вымогателей, шпионских программ, вредоносных программ, фишинга, несанкционированного сбора данных и профилирования.

Использование системы управляемой передачи файлов для защиты ваших данных

Проблема:

Отсутствие системы, позволяющей автоматизировать бизнес-сценарии при передаче файлов между организацией и её контрагентами. Передача данных осуществляется на основе небезопасных и/или устаревших протоколов.

Данные, которые должным образом не зашифрованы, могут быть скомпрометированы. Только в этом году в банке «Скоттрейд» (Scottrade) произошла утечка из базы данных, содержащей данные 20 000 клиентов. База данных не была зашифрована и были украдены учетные данные, номера социального страхования, имена и другие персональные данные сотрудников. Обидно, что всего этого можно было бы избежать, ис-

пользуя практики кибербезопасности и планирование.

Защитите каждый файл, папку и базу данных в общедоступных и частных сетях с помощью шифрования, применяя алгоритмы AES и OpenPGP и протоколы и SFTP, FTPS, AS2 и HTTPS при передаче данных.

Решение:

Внедрите систему управляемой передачи файлов (Managed File Transfer — MFT) в своей организации.

Что такое управляемая передача файлов (MFT)?

MFT появилось для удовлетворения растущих потребностей организаций, которые хотели сократить свои затраты на передачу файлов, значительно улучшить свою кибербезопасность и заменить использование уязвимых протоколов передачи файлов, таких как FTP.

По сути, это технология «все-в-одном», которая автоматизирует и шифрует передачу файлов. MFT позволяет администраторам выполнять следующие задачи:

- Шифровать и дешифровать конфиденциальные файлы и документы
- Осуществлять передачу пакетных файлов по расписанию
- Запускать рабочие процессы для обработки завершенных передач
- Связываться с торговыми партнерами с помощью внешних серверов или облака
- Просмотр журналов аудита для получения важных сведений о передачах
- Создание отчетов для ключевых заинтересованных сторон

Решение MFT упрощает выполнение критически важных бизнес-задач и сокращает время, затрачиваемое на ручную передачу файлов, пользовательские сценарии, внутренние процессы и многое другое. Благодаря MFT организации могут быть уверены в том, что их бизнес-процессы будут работать бесперебойно и эффективно, без задержек, ошибок или уязвимостей.

Вот несколько признаков того, что имеет смысл рассмотреть возможность внедрения решений MFT.

1. Необходимо провести аудит операций передачи файлов

В некоторых распространенных сценариях может потребоваться аудит передачи файлов. Возможно, ваши торговые партнеры и заинтересованные стороны хотят получить обзор деятельности за месяц. Или, возможно, передача файлов не удалась, и вам нужно выяснить, где произошел сбой. Независимо от ситуации, MFT хранит подробные логи для всех операций передачи файлов и рабочих процессов, которые когда-либо выполнялись.

Некоторые решения имеют интерфейс, который позволяет быстро искать в журналах конкретные термины, пользователей или диапазоны дат. Также можно изучить процессы передачи файлов, чтобы получить детали из журнала заданий, в том числе время и дату начала работы, частью какого проекта она была, и был ли удачен тот или иной этап проекта.

2. Для отправки данных используются традиционные методы

С 1970-х годов протокол FTP позволяет организациям быстро отправлять и извлекать данные. Он по-прежнему популярен; несмотря на то, что появились новые протоколы передачи файлов, которые обеспечивают шифрование, многие ИТ-команды по-прежнему предпочитают использовать FTP для своих нужд.

Кибератаки проверяли целостность FTP-связи на протяжении многих лет. Поскольку FTP устарел и не соответствует современным стандартам безопасности, это плохой выбор для отправки файлов через частные и/или общедоступные сети. Может возникнуть соблазн отправлять данные с помощью доморощенных решений, однако использование старых технологий отнимает много времени, их трудно поддерживать, и они полны недостатков и уязвимостей. Использование любого из этих методов (FTP и ручные процессы) может привести к утечке данных.

С другой стороны, MFT снимает с Вас риски, техническое обслуживание и работы по программированию. Управляемая передача файлов легко поддается аудиту, удобна в использовании, и дает возможность планировать пакетные передачи и снимает часть нагрузки с ИТ отдела. Более того, все MFT решения поддерживают протоколы для безопасного обмена данными — SFTP, FTPS и HTTPS, все они обеспечивают шифрование; в отличие от обычного FTP.

3. Процессы должны адаптироваться к изменяющимся условиям сети

Предсказать и предотвратить простой очень сложно, особенно в случае непредвиденной ошибки или стихийного бедствия. Но возможно подготовиться подобным сбоям, обеспечив максимально высокую до-

ступность критически важных систем передачи файлов и серверов.

Такие решения, как MFT, предоставляют методы кластеризации active-passive и active-active, а также катастрофоустойчивые конфигурации и возможность применения технологии DR (Disaster Recovery — Восстановление после сбоя) для организаций, которым необходимо поддерживать свои процессы в активном состоянии независимо от ситуации. Кластеризация обеспечивает наилучшую отказоустойчивость за счет одновременного запуска нескольких серверов. Если один падает, то передачи файлов и рабочие процессы будут выполняться на других серверах поэтому связь с сотрудниками и торговыми партнерами не будет нарушена.

4. Вы должны соответствовать государственным требованиям

Некоторые компании работают с правительственными организациями. Таким образом, они должны соответствовать специальным требованиям по отчетности и шифрованию. С помощью MFT эти требования могут быть выполнены следующим образом:

- ГОСТ 28147–89 совместимые алгоритмы шифрования.
- Журналы аудита и созданные отчеты
- Безопасная аутентификация и контроль пользователей

10. Создание и внедрение программы повышения осведомленности о безопасности

Проблема:

Целенаправленный фишинг остается одним из наиболее часто используемых способов хищения конфиденциальной информации компании. Это тревожный факт; с учетом того, что средняя стоимость утечки данных составляет более 3 миллионов долларов, ставки слишком высоки для вредоносного электронного сообщения, вызывающего проблемы у клиентов и учреждений. Но утечки в результате целенаправленного фишинга можно полностью предотвратить.

Ни для кого не секрет, что человеческий фактор самая большая уязвимость для компаний, ведущих борьбу с фишингом. Интернет-сообщество профессионалов в области безопасности Dark Reading объясняет эту загадку на своем брифинге по недавнему исследованию инструмента рассылки фишинговых писем по электронной почте PhishMe: «Отчет показал, что 91% кибератак начинаются с фишинговых писем, и основные причины, по которым люди ведутся на такие письма — это любопытство, страх и спешка» [4].

Банки не защищены от такого поведения. Например, Банк Канады (Bank of Canada) не смог удержать своих сотрудников от чтения подозрительных писем или запуска подозрительных приложений. Financial Post пишет, что «люди являются слабым звеном в кибербезопасности центрального банка. Помимо сотрудников, которых подтолкнули к открытию вредоносных писем, были еще и пользователи, которые загружали вредоносное программное обеспечение во время серфинга в Интернете или просмотра онлайн магазинов и отправляли его по электронной почте на рабочие адреса».

Решение:

Большинство людей знают, что не нужно нажимать на подозрительные ссылки или открывать вложения от «иностранных принцев» и учреждений, в которых они никогда не делали покупки, но хакеры стали также умны, как и мы. Большинство вредоносных программ и афер скрыты за сообщениями от достоверных отправителей, таких как генеральный директор компании или бухгалтерия.

Сделайте кибербезопасность основным направлением в вашей организации. Определите стратегию и хорошую программу повышения осведомленности о безопасности, а затем реализуйте ее, начиная с процесса обучения каждого сотрудника. Требуйте проведения частых тренингов, чтобы вся компания была осведомлена о новейших слабых местах и политиках безопасности, но следите, чтобы это было увлекательно. Чем больше сотрудников чувствуют себя наделенными полномочиями и вовлеченными в успех организации, тем больше будут соблюдать надлежащие меры безопасности.

5. Источником почти всех успешных атак является общедоступный интернет, а атаки через браузеры составляют основную часть атак против пользователей.

Проблема:

Неосведомленность специалистов в области ИТ о проблемах информационной безопасности, связанных с браузерами конечных пользователей. Со временем браузеры становятся мишенью вредоносного ПО, программ-вымогателей и других видов небезопасного ПО. Добавьте ко всему этому пользователей, которые слишком вольно обращаются с клавиатурой или с мышкой, так называемых happy clickers, а также среду, в которой отсутствует регулярное обновление и корректировка браузеров — и в результате получаем просто катастрофическую ситуацию для информационной

безопасности. Все данные факторы добавляют к уже опасной самой по себе среде браузеров несметное количество векторов угроз.

Решение:

Дело в том, что на самом деле очень легко устранить данные проблемы. Для начала необходимо запретить использование браузеров. Несомненно, у читателя эти слова вызовут шок. Тем не менее, проблема была бы решена, но, по всей видимости, это в принципе невозможно.

В таком случае как предприятия могут обеспечить надлежащий уровень безопасности, масштабируемости, работоспособности и высокую степень прозрачности в сложной сетевой среде? Ответ прост — применить технологию изоляции браузера или так называемый воздушный зазор.

Понятно, что пока навигация не будет очищена от угроз, предприятия будут подвергаться риску, связанному с множеством проблем в области безопасности.

Изоляция браузера работает с использованием того же метода, что и больница, изолирующая инфекционного пациента от остальной части здорового населения.

До тех пор, пока сохраняется инфекция, семья и друзья могут общаться с инфекционными пациентами через окна и динамики, благодаря чему обеспечивается защита от опасных микроорганизмов. Когда пациент вылечится, он выходит из изолятора. Его изоляционная камера быстро возвращается в первоначальное стерильное состояние и готова к приему следующего пациента: зараженные предметы утилизируются, а поверхности подвергаются обработке, причем опасные возбудители уничтожаются до возможного распространения за пределы данной камеры.

Аналогичным образом благодаря изоляции процесса навигации, связанные с рисками сеансы, прообразовываются для пользователей в безопасный визуальный поток без вредоносных программ. В случае необходимости элементы для загрузки при доставке полностью «дезинфицируются» с помощью технологии санитизации. И как только потребность в изоляции отпадает, в отличие от дорогостоящего медицинского оборудования, удаленные изолированные браузеры просто уничтожаются вместе со всеми инфекционными вредоносными программами, приобретенными во время сеанса, и для следующего сеанса навигации создается новый браузер.

Добавляя такой уровень изоляции, предприятия устанавливают барьер между конечными устройствами и небезопасной зоной сети Интернет. Изоляция никак не отображается на использовании браузера пользователями, но при этом значительно сводятся к минимуму риски атак и вредоносных инфекций.

Изоляция браузеров обладает немалым количеством преимуществ:

- Минимизация количества векторов атак. Несмотря на то, что изолирование и надежная защита браузеров не могут полностью исключить веб-атаки, количество векторов атак при этом существенно уменьшается.
- Упрощение эффективного управления. Не во всех организациях имеется централизованный сервер обновления, который гарантирует развертывание обновления браузера в рамках всей организации. Изоляция браузера означает, что больше не надо беспокоиться о том, какую версию Firefox, IE или Chrome используют сотрудники. Достаточно одного обновления — и дело в шляпе.
- Обеспечение всесторонней защиты. Предполагается концепция информационной безопасности, согласно которой на предприятии внедряются несколько уровней элементов управления безопасностью. Таким образом обеспечивается наличие альтернативных средств в случае сбоя системы безопасности или проявления уязвимости, благодаря чему исключаются точки отказа, которые подвергают сеть широкомасштабным атакам. Изоляция является дополнением к набору средств обеспечения информационной безопасности.
- Возможность интеграции с другими решениями. Изоляция браузера дополняет существующие основные решения в области обеспечения безопасности, такие как безопасные интернет-шлюзы (SWG), брандмауэры, системы обнаружения вторжений (IDS), предотвращения потери данных (DLP) и мониторинга целостности файлов (FIM). Кроме того, удаленная изоляция расширяет существующие средства классификации.
- Минимизация расходов на техническую поддержку. Изоляция браузера сводит к минимуму различия в настройках навигации у сотрудников. При обращении в службу технической поддержки много времени уходит на то, чтобы понять, что происходит с конфигурацией и настройками браузера конечного пользователя. Если данный элемент устранить, обращения в службу поддержки будут занимать меньше времени, расходы сократятся, а производительность увеличится, что является веским преимуществом.

ЛИТЕРАТУРА

1. https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85 (дата обращения: 17.04.22).
2. https://www.paymentssource. com/opinion/a-culture-of-security-can-harden-a-companys-defenses (дата обращения: 18.04.22).
3. https://www.securelink.com/blog/breaches-two-factor-authentication-blocked/ (дата обращения: 17.04.22).
4. https://www.darkreading.com/attacks-breaches/hackers-and-artificial-intelligence-a-dynamic-duo/d/d-id/1335741(дата обращения: 17.04.22).
5. https://www.darkreading.com/vulnerabilities—-threats/a-new-risk-vector-the-enterprise-of-things-/a/d-id/1339081
6. https://www.interfax.ru/russia/680021(дата обращения: 17.04.22).
7. «Проблемы Квалификации Хищения Электронных Денежных Средств» Алехин Виталий Петрович, Булавка Дмитрий Михайлович. Кубанский государственный аграрный университет имени И.Т. Трубилина, г. Краснодар, Россия. Тип: статья в журнале — научная статья Язык: русский. Номер: 34 Год: 2019 Страницы: 20–25. УДК: 343.72 (дата обращения: 18.04.22).
8. «Способ И Цель Совершения Мошенничества» Хоменко Анатолий Николаевич, Черемнова Наталья Александровна НОУ ВПО «Сибирский институт бизнеса и информационных технологий» Омской академии Министерства внутренних дел Российской Федерации. Тип: статья в журнале — научная статья Язык: русский. Номер: 4 (28) Год: 2018 Страницы: 95–99 Поступила в редакцию: 22.11.2018.УДК:343.721.https://elibrary.ru/download/elibrary_32722868_61561257.pdf (дата обращения: 17.04.22).

Журнал «Современная наука: актуальные проблемы теории и практики»

Московский Государственный Технический Университет им. Н.Э. Баумана