Научная статья
Original article
004.424

ЗАЩИЩЕННОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

SECURITY OF INFORMATION SYSTEMS

Кодацкий Никита Максимович, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), nickitadatsky@gmail.com
Камбулов Данил Александрович, магистр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), kambulov18@yandex.ru

Kodatsky Nikita Maksimovich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), nickitadatsky@gmail.com
Kambulov Danil Alexandrovich, Master, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), kambulov18@yandex.ru

Аннотация: в данной статье описаны методы раскрытия и сокрытия личностных данных в различных информационных средах. Обычный пользователь все чаще и чаще прибегает новым версиям программного продукта, забывая о том, что самые популярные программы - это большие носители ошибок. Только для каждого приложения Microsoft каждый месяц выходят приложения с исправлениями тех или иных неполадок. Интернет все чаще становится более приемлемым средством для связи с экспертами тех или иных областей. Но в нем все больше «хакеров», так или иначе «бьющихся» за

интересную информацию. Так что актуальность защиты информации стоит на одном из первых мест.

Abstract: this article describes the methods of disclosure and concealment of personal data in various information environments. An ordinary user more and more often resorts to new versions of a software product, forgetting that the most popular programs are big carriers of errors. Only for each Microsoft application, applications are released every month with fixes for certain problems. The Internet is increasingly becoming a more acceptable means of communication with experts in various fields. But there are more and more "hackers" in it, one way or another "fighting" for interesting information. So the relevance of information protection is one of the first places.

Ключевые слова: информационная безопасность, защита данных, техническое обслуживание

Keywords: information security, data protection, maintenance

Компьютерные технологии изменили нашу жизнь. Почти весь мир не представляет жизнь без информационных технологий. Сегодня почти во всех отраслях проектируется информационные системы, объединяющиеся в единую систему с помощью локальной и /или глобальной системой. При этом никто не задумывается о том, что персонализация данных может привести к правонарушению. Предпосылкой к этому:

— Не защищенность информации, открытость оборудования с информацией требующей защиту.

— Не проведение технического обслуживание объектов (дефрагментация, очистка дисков, исправление ошибок на диске, прослеживание и удаление дублированных файлов, тестирование операционной системы, замена устаревшего оборудования и т.д.)

— многие законодательные акты требуют усовершенствования, в том числе в вопросах государственной, личной тайны и в защите медицинских компьютерных технологий и информационных технологий в целом.

К безопасности необходимо подходить с нескольких сторон:

Технической: Защита информации стала одной из главных проблемой в современном обществе. Так для медицинских учреждений проектируется программное обеспечение для различных аппаратов, а об их обслуживании все забывают после продажи. Либо многие программы не доведены до логического конца, что доставляет значительные трудности в эксплуатации (например, Анализатор иммуноферментных реакций АИФР-01 фирмы «Пикон»). Но нельзя забывать о техническом состоянии устройств, обращающихся к информации. Необходимо создать должность в организациях, которая беспрепятственно выполняла бы роль «дворников» для компьютеров. Но необходимо не забывать о сохранности данных…

Программной: ФИО, паспортные данные встречаются почти в каждой базе данных. На мой взгляд, уже должен выработаться стандарт заполнения баз, который привел бы к заполнению единой базы. Так, например, в медицинском учреждении заполняются данные касающиеся здоровья, а в банке, касающиеся денежного состояния, шифровался и локально заносился в память.

Юридической: необходимы юридические рекомендации для каждой области данных по созданию защищенной базы с созданием практических рекомендации по организации защитных мероприятий технической сферы.

Название «Magecart» относится к нескольким группам хакеров, которые используют методы онлайн-скимминга с целью кражи личных данных с веб-сайтов - чаще всего данных о клиентах и информации о кредитных картах на веб-сайтах, которые принимают онлайн-платежи. Группы Magecart успешно взломали известные бренды. Название навеяно изначальной целью этих групп - платформой Magento, которая обеспечивает функции оформления заказа и корзины покупок для сайтов розничных продавцов.

Влияние атак Magecart

Вот несколько возможных последствий атак Magecart:

- **Кража личной информации -** хотя основной целью атак Magecart является информация о кредитных картах, злоумышленники также могут украсть личную информацию. Это потенциально может повлиять на миллионы покупателей.
- **Потеря доходов** - розничный торговец электронной коммерцией малого и среднего размера, ранее взломанный Magecart, может увидеть значительное снижение онлайн-продаж. Это связано с тем, что покупатели могут потерять доверие к способности продавца предотвратить новое нарушение.
- **Дальнейшее заражение -** если группа Magecart извлекает учетные данные пользователя и учетные данные администратора, они потенциально могут расширить атаку, чтобы заразить дополнительные сайты. Например, во время взлома VisionDirect.co.uk группа Magecart заразила не только основной сайт, но и розничные сайты семи других европейских стран.
- **Юридические и нормативные убытки** - атака Magecart подвергает компанию судебным искам со стороны затронутых клиентов, судебным санкциям, если компания подчиняется правилам, таким как GDPR , и отраслевым штрафам, таким как аудит PCI DSS и невозможность обрабатывать кредитные карты.

Примеры жертв Magecart

Вот несколько ярких примеров организаций, которые стали мишенью групп Magecart.

Magento

Первоначально Magecart нацелился на Magento - стороннюю программу для покупок. Название Magecart представляет собой комбинацию «корзина для покупок» и «Magento», и по сей день Magento и другие поставщики программного обеспечения для электронной коммерции, такие как OpenCart, в первую очередь нацелены на группы Magecart.

British Airways

British Airways опубликовала информацию о взломе ее веб-сайта и мобильного приложения. Злоумышленникам удалось украсть платежную информацию 380 000 клиентов British Airways.

Согласно RiskIQ, взлом совершил Magecart. Злоумышленники смогли напрямую взломать веб-сайт British Airways, воспользовавшись его уникальной функциональностью и структурой.

Злоумышленники Magecart скопировали платежные формы JavaScript с веб-сайта British Airways, а затем изменили форму, чтобы она отправляла платежную информацию на сервер, контролируемый участниками. Чтобы избежать обнаружения, субъекты следили за тем, чтобы формы продолжали работать, как задумано в браузерах конечных пользователей.

Кроме того, актеры знали, что мобильное приложение British Airways также использовалось аналогично тому, что использовалось в веб-приложении. Это означает, что, взломав веб-сайт, участники также могут получить доступ к мобильному приложению. Многие из 380 000 жертв на самом деле были пользователями мобильных приложений.

Корзины Amazon S3

RiskIQ обнаружил, что группа Magecart скомпрометировала намного больше сторонних веб-поставщиков, чем сообщалось ранее. Фактически было обнаружено, что эти субъекты фактически автоматизировали процесс взлома веб-сайтов с помощью скиммеров. Они достигли этого за счет упреждающего сканирования на предмет неправильно настроенных корзин Amazon S3, а затем взломали значительное количество корзин S3, которые затронули более 17 000 доменов - многие из этих веб-сайтов даже входят в топ 2 000 рейтинга Alexa.

Ханна Андерсон

В 2020 году американский производитель детской одежды и онлайн-продавец Ханна Андерссон сообщила, что ее платформа онлайн-покупок для электронной коммерции была взломана, и в течение почти двух месяцев был внедрен вредоносный код для кражи платежной информации клиентов.

Как это часто бывает с атаками Magecart, эта атака оставалась незамеченной, пока украденные кредитные карты не появились в даркнете. В результате нарушения Ханна Андерссон согласилась выплатить 400 тысяч долларов в судебном иске, касающемся Закона о защите прав потребителей Калифорнии (CCPA). Согласно соглашению, более 200 000 клиентов из США, которые сделали покупки в интернет-магазине Hanna Andersson с 16 сентября по 11 ноября 2019 г., имеют право на получение компенсации по соглашению.

Как работают атаки Magecart?

Каждая группа Magecart может действовать по-своему. В предыдущих атаках использовались разные шаблоны, в том числе:

- Ориентация в первую очередь на небольшое количество ценных организаций.
- Массовые атаки созданы специально для атаки как можно большего числа поставщиков.
- Использование нескольких различных типов инъекций и скиммеров кода , а также других методов вторжения и множества дополнительных тактик и инструментов.
- Проведение атак на цепочку поставок, нацеленных на сторонних поставщиков, которые могут предоставить доступ к нескольким веб-приложениям.
- Ориентация на платформы электронной коммерции.

Хотя каждая группа может выбирать разные цели и тактику, большинство из них используют формджекинг или цифровой скимминг, чтобы украсть информацию о платежных картах посетителей веб-сайта.

Недавние исследования показали, что с помощью formjacking приходится почти 3/4 утечек данных, связанных с Интернетом, причем половина из них затрагивает отрасль розничной торговли.

Еще один важный аспект атак - постоянная угроза Magecart. Исследователи безопасности обнаружили, что один из пяти магазинов

электронной коммерции, ранее зараженных Magecart, повторно заражается в течение нескольких дней. Оперативники Magecart часто:

- Заполните взломанные магазины множеством бэкдоров, включая мошеннические учетные записи администраторов.
- Используйте различные механизмы повторного заражения, включая скрытые периодические задачи и триггеры базы данных, которые позволяют им восстановить свою полезную нагрузку.
- Используйте методы запутывания, которые помогают сделать их присутствие неотличимым от легитимного кода.
- Используйте уязвимости нулевого дня , для которых нет исправлений, для взлома сайтов.

Защита от атак Magecart

Что могут сделать торговцы, чтобы предотвратить атаки Magecart?

Чтобы снизить риск Magecart и других типов атак на стороне клиента, выполните следующие действия:

- **Определите сторонний JavaScript** - подготовьте инвентаризацию всего стороннего кода JavaScript на вашем веб-сайте.
- **Попросите сторонних поставщиков провести аудит их кода,** чтобы убедиться, что это их исходный код и не содержит вредоносных инструкций или вредоносных программ.
- **Переключитесь со сторонних служб на сторонние** - по возможности лучше запускайте программное обеспечение на своих серверах и не используйте сторонние службы. Это может оказаться проблемой, поскольку сегодня большинство витрин в значительной степени зависят от сторонних поставщиков.
- **Внедрение заголовков HTTP Content-Security-Policy** - обеспечивает дополнительный уровень защиты от межсайтовых сценариев (XSS), кликджекинга и других атак путем внедрения кода.

Сегодня существуют специализированные решения, которые обеспечивают защиту на стороне клиента и помогают предотвратить атаки Magecart.

Что потребители могут сделать, чтобы защитить себя?

Покупая в Интернете, потребители доверяют веб-сайтам электронной коммерции. Хотя продавцы электронной коммерции несут ответственность за безопасность своего сайта, существуют меры, которые может принять каждый отдельный потребитель. Потребители должны рассмотреть возможность применения следующих мер безопасности:

- **Избегайте ввода личной информации** на веб-сайтах, которым они не доверяют.
- **Используйте такую службу, как privacy.com,** для создания одноразовых кредитных карт.
- **Проверьте URL-адрес домена,** чтобы убедиться, что это не поддельный домен с аналогичным именем, созданный злоумышленниками.
- **Используйте плагины браузера,** чтобы предотвратить загрузку JavaScript с ненадежных сайтов. Это может помочь уменьшить поверхность атаки. Обратите внимание, что этот метод не может защитить от вредоносного кода, который уже встроен в доверенные сайты.
- **Блокируйте подключения** к IP-адресам и доменам, которые, как известно, используются злоумышленниками. Это может быть настроено администраторами на корпоративных или управляемых устройствах.

Список литературы

1. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. — М.: КноРус, 2016. — 136 с.
2. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

3. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 с.
4. Ефимова, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. — М.: ЮНИТИ-ДАНА, 2016. — 239 с.

References

1. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. — M.: KnoRus, 2016. — 136 p.
2. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2017. - 324 p.
3. Gromov Yu.Yu. Information security and information protection: Textbook / Yu.Yu. Gromov, V.O. Drachev, O.G. Ivanova. - Art. Oskol: TNT, 2017. - 384 p.
4. Efimova, L.L. Information security of children. Russian and foreign experience: Monograph / L.L. Efimova, S.A. Poker. — M.: UNITI-DANA, 2016. — 239 p.

© Кодацкий Н.М., Камбулов Д. А., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Кодацкий Н.М., Камбулов Д. А. ЗАЩИЩЕННОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ // Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.