Научная статья
Original article
УДК 004

КАК ПРЕДОТВРАТИТЬ УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

HOW TO PREVENT PERSONAL DATA LEAKAGE

Коломыцев Александр Сергеевич, студент Балтийский федеральный университет Им. И. Канта (236041 Россия, г. Калиниград, ул. Александра невского, д. 14), тел. 8(963)268-55-54, tzhz@mail.ru

Вердиев Орхан Ровшанович, студент Балтийский федеральный университет Им. И. Канта (236041 Россия, г. Калиниград, ул. Александра невского, д. 14), тел. 8(913)039-86-98, orhan-rv@mail.ru

Kolomytsev Alexander Sergeevich, student of the Baltic Federal University. I. Kant (236041 Russia, Kaliningrad, Alexander Nevsky St., 14), tel. 8(963)268-55-54, tzhz@mail.ru

Verdiev Orkhan Rovshanovich, student of the Baltic Federal University. I. Kant (236041 Russia, Kaliningrad, Alexander Nevsky St., 14), tel. 8(913)039-86-98, orhan-rv@mail.ru

Аннотация. Утечка данных является проблемой не только для компаний, но и для обычных людей. В этой статье рассматриваются варианты защиты своих персональных данных, а также описание действий для предотвращения утечки.

Abstract. Data leakage is a problem not only for companies, but also for ordinary people. This article discusses options for protecting your personal data, as well as a description of actions to prevent leakage.

Ключевые слова. Утечка данных, персональные данные, VPN, SSL, файервол, бэкап., даркнет, безопасность данных, защита сервера.
Keywords. Data leakage, personal data, VPN, SSL, firewall, backup, darknet, data security, server protection.

Нарушение данных - это нарушение безопасности, при котором конфиденциальные, защищенные или конфиденциальные данные копируются, передаются, просматриваются, крадутся или используются лицом, не уполномоченным на это.

Существует много разных факторов утечки персональных данных. Основные из них:

1. от безалаберности сотрудников/разработчиков: открытые БД, открытые порты и т.п.;
2. слив данных самими сотрудниками;
3. дыры безопасности сайтов.

Также утечку данных можно разделить на два больших вида: умышленная и неумышленна. Чаще всего не умышленные утечки данных происходят в сфере медицинских услуг [1]. На долю здравоохранения приходится до 60% утечек произошедших по вине сотрудников и только 20% сделаны умышленно, остальные произошли из-за не компетенции сотрудников. Также большой процент не умышленных утечек данных происходит в сферах образования и ЖКХ. Но если говорить в общем то в мире 72% [2] утечек данных происходит умышленно. Чаще всего атакам подвергаются государственные учреждения, банки, страховые организации.

Утечки персональных данных ведут к повышению активизации мошенников. Также часто утечки могут быть использованы в маркетинговых целях. Выглядит это так: человек провести небольшое исследование, собирает слитые данные с нескольких сервисов, и по ним составляет профиль человека. Это помогает узнать, что это человек любит есть, где бывает и что смотрит.

Когда у злоумышленников/продажников и тд. есть такой портрет, можно выявить боли человека и знать куда “давить”.

Найти слитые данные можно в даркнете [3]. Даркнет — это скрытый сегмент интернета, доступный только через специализированные браузеры. Для безопасности пользователей сети даркнет полностью анонимен — для доступа к нему используется зашифрованное соединение между участниками.

Еще один набирающий популярность способ “пробить человека” различные Telegram-каналы или боты, где за небольшую плату можно получить необходимую информацию, просто предоставив ФИО или номер телефона. Существую два типа работы таких сервисов:

- Схема OSINT [4], то есть опираются на открытые и доступные источники. Для этого они используют API различных служб и интернет-ресурсов.
- Слитые базы данных. Такой способ менее достоверный, так как существует проблема актуализации информации.

Мы как пользователи тех или иных сервисов часто даем согласие на обработку персональных данных при получении определенных услуг, при покупке товаров через онлайн-сервис и так далее.

Порядок работы с личными нашими сведениями установлен законом «О персональных данных» от 27.07.2006 № 152-ФЗ [5]. Из статьи 3 закона следует, что к индивидуальным данным лица относится любая информация о нем, позволяющая его идентифицировать.

В том числе к таким сведениям можно отнести:

- Ф. И.О.;
- адрес проживания;
- паспортные данные;
- сведения о месте рождения;
- прочие данные.

Согласно статьи 9 вышеуказанного закона [5] можно отзывать согласие на обработку персональных данных, что позволяет наложить запрет на работу оператора с личными сведениями о человеке.

Между тем оператор может продолжить работу с личными инфоматериалами субъекта даже при отзыве последним своего согласия. Перечень случаев, когда у него есть такое право, прописан в пп. 2–11 ч. 1 ст. 6, ч. 2 ст. 10, ч. 2 ст. 11 закона № 152-ФЗ [5]. В частности, использовать информацию о человеке могут:

- суды при участии гражданина в судопроизводстве;
- приставы при исполнении судебного акта;
- государственные органы при исполнении своих полномочий;
- стороны гражданско-правовых договоров, заключенных с субъектом персональных данных;
- любые субъекты при необходимости защиты жизни или здоровья носителя персональной информации;
- журналисты, если работа с личной информацией связана с их профессиональной деятельностью;
- субъекты, участвующие в реализации международных договоров;
- органы статистики, если личные данные обезличиваются.

Есть еще несколько видов, как можно «убрать» данные из интернета.

Можно запретить поисковым системам их отображать в поиске. В федеральном законодательстве говорится о праве на забвение [6], позволяющее гражданам обращаться с заявлением о прекращении выдачи в поисковике личных данных. Суть заключается в следующем: каждый человек может обратиться к администрации поисковика и попросить удалить ссылки на его страницы из списка поиска. Поисковик перестанет показывать эту информацию, но информация, конечно, останется и найти ее уже сможет только тот, кто знает конкретный адрес. Можно попросить “удалить” информацию, которая явно наносит вред чести и достоинству заявителя, а также можно удалить неактуальную информацию. Уточнение: закон не

распространяется на внутренний поиск по соцсетям и для каждого поисковика есть свои собственные статьи, поэтому при подходе к данному вопросу стоит хорошо изучить информацию [6].

Если же Вы обнаружите свои персоналии на каком-либо сайте, необходимо сообщить об этом администратору, модератору или владельцу веб-ресурса (отправить электронное письмо по реквизитам сайта). То есть требовать, чтобы сведения удалили или хотя бы обезличили.

Еще один вариант, который может помочь - подать в суд на компанию которая слила эти самые данные.

Безопасность данных это необходимость. Не важно на чем они хранятся: сайты, мобильные приложения, компьютеры или телефонов, все сводится к защите сервера.

Защита сервера от взлома - мера комплексная. Ниже приведен список мер, который поможет защитить сервер от взлома.

Использование SSH-ключа предлагается в качестве альтернативы паролю. SSH-ключ имеет длину больше, чем пароль, а также состоит из открытой и закрытой части [8]. Открытая кладётся в домашний каталог пользователя, «которым» заходят на сервер, закрытая — в домашний каталог пользователя, который идёт на удалённый сервер.

Файервол - это система, которая предотвращает несанкционированный доступ к сети, «межсетевой барьер», который при помощи контроля трафика, блокирует доступ к нежелательному контенту.

Virtual Private Network (VPN) – технология, благодаря которой можно создать безопасное подключение пользователя к сети. Чаще используется для обхода ограничений.

TLS — протокол установления и использования криптографически безопасного соединения между клиентом и сервером по сети Интернет. Он дает возможность клиентам проводить проверку подлинности серверов [7].

Серверы же с его помощью выполняют проверку подлинности клиентов (когда это важно).

SANDBOX. Благодаря виртуализации, все процессы, инициированные программой, выполняются в песочнице — изолированной среде с жестким контролем системных ресурсов.

Дополнительные блокировщики - локальные сервисы, которые отслеживают log–файлы запущенных программ, и на основании различных условий блокирует по IP найденных нарушителей.

Настройка резервного копирования, позволяет держать копии на другом диске [8]. Данная мера не является защитой от взлома, по помогает избежать потери данных.

Двухфакторная аутентификация. При таком типе аутентификации вы подтверждаете вход двумя типами. Чаще всего это пара логин/пароль + код.

Список литературы

1. Tadviser. Утечки данных в медицинских учреждениях 31.12.2021 [Электронный ресурс] // https://www.tadviser.ru/index.php/Статья:Утечки_данных_в_медицинских_учреждениях
2. Tadviser. Утечки данных 6.04.2022 [Электронный ресурс] // https://www.tadviser.ru/index.php/Статья:Утечки_данных
3. Даркнет уже не тот. Что дешевеет, а что дорожает на подпольном онлайн-рынке // Коммерсантъ от 30.05.2020
4. Киви Бёрд. Модель OSINT // Компьютера. — 06.07.2007
5. КонсультантПлюс. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ
6. КонсультантПлюс. Федеральный закон "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и статьи 29 и 402 Гражданского процессуального кодекса Российской Федерации" от 13.07.2015 N 264-ФЗ

7. Александр Венедюхин, Ключи, шифры, сообщения: как работает TLS (Техническое описание TLS), 04/09/2015
8. Eric Cole. Руководство по защите от хакеров 640 стр., с ил.; ISBN 5-8459-0278-9, 0-7357-1009-0; Вильямс.
9. Комер, Дуглас Э.; Стивенс, Дэвид Л. (1993). Том III: Клиент-серверное программирование и приложения. Межсетевое взаимодействие с TCP/IP. Департамент компьютерных наук, Университет Пердью, Уэст-Лафайет
10. Терри Оглтри. Модернизация и ремонт сетей = Upgrading and Repairing Networks. — 4-е изд. — М.: «Вильямс», 2005. — С. 1328
11. Джеймс Ф. Куросе, Кит В. Росс, Компьютерные сети: нисходящий подход, 2008 г.

References

1. Tadviser. Data leaks in medical institutions 12/31/2021 [Electronic resource] // https://www.tadviser.ru/index.php/ Article: Data_leaks_in_medical_institutions
2. Tadviser. Data leaks 04/06/2022 [Electronic resource] // https://www.tadviser.ru/index.php/ Article: Data_leaks
3. The darknet is no longer the same. What is getting cheaper and what is getting more expensive in the underground online market // Kommersant from 05/30/2020
4. Kiwi Bird. OSINT Model // Computer. — 07/06/2007
5. ConsultantPlus. Federal Law "On Personal Data" dated July 27, 2006 N 152-FZ
6. ConsultantPlus. Federal Law "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" and Articles 29 and 402 of the Civil Procedure Code of the Russian Federation" dated July 13, 2015 N 264-FZ
7. Alexander Venedyukhin, Keys, ciphers, messages: how TLS works (TLS White Paper), 04/09/2015

8. Eric Cole Hacker Protection Guide 640 pp., with illustrations; ISBN 5-8459-0278-9, 0-7357-1009-0; Williams.
9. Comer, Douglas E.; Stevens, David L. (1993). Vol III: Client-Server Programming and Applications. Internetworking with TCP/IP. Department of Computer Sciences, Purdue University, West Lafayette
10. Terry Ogletree. Upgrading and Repairing Networks = Upgrading and Repairing Networks. - 4th ed. - M .: "Williams", 2005. - S. 1328
11. James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 2008

© Коломыцев А.С., Вердиев О.Р., 2022 Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.

Для цитирования: Коломыцев А.С., Вердиев О.Р. КАК ПРЕДОТВРАТИТЬ УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №7/2022.