Автор: Артур Скальский ИНТЕРНЕТ И ИТ, МИР

Эксперты: утечка данных через поисковики - вина разработчиков сайтов

Причиной попадания данных пользователей различных интернет-сервисов в поисковую выдачу является человеческий фактор, - как правило, это ошибки разработчиков и администраторов сайтов, рассказали РИА Новости опрошенные во вторник эксперты.

Причиной попадания данных пользователей различных интернет-сервисов в поисковую выдачу является человеческий фактор, - как правило, это ошибки разработчиков и администраторов сайтов, рассказали РИА Новости опрошенные во вторник эксперты.

За минувшие десять дней в рунете произошли сразу три крупных утечки информации через поисковые системы. 18 июля в выдачу популярных поисковиков, в частности, "Яндекса", попали тексты SMS, отправленные с сайта компании "МегаФон", а также номера телефонов получателей.

Спустя неделю в поисковой выдаче были обнаружены ссылки на страницы со статусами заказов в различных интернет-магазинах. На этот раз в открытый доступ попали электронные адреса покупателей, перечень заказанных товаров, сумма покупки, адрес доставки и IP-адрес устройства, с которого был сделан заказ. По данным Роскомнадзора, были скомпрометированы клиенты более чем 80 интернет-магазинов.

Во вторник в поисковой выдаче оказались электронные железнодорожные билеты с датами, номерами рейсов, именами пассажиров. Если сведения о проездных документах подлинные, это, как и в случае с публикацией информации о клиентах интернет-магазинов, означает утечку персональных данных.

В пресс-службе "Яндекса" РИА Новости сообщали, что первые две утечки связаны либо с отсутствием, либо с некорректным использованием на сайтах файла robots.txt, который содержит описание правил индексирования для поисковых роботов.

Эксперты, опрошенные РИА Новости, полагают, что инциденты стали следствием халатности разработчиков и администраторов сайтов.

На совести разработчиков

По словам специалиста по компьютерной криминалистике Group-IB Сергея Никитина, последние крупные утечки произошли по двум причинам. "Во-первых, страницы находились в публичном, т.е. открытом, доступе. Во-вторых, не было верно задано правило для поисковых роботов: не индексировать данные страницы", - рассказал РИА Новости Никитин.

Эксперт также сообщил, что при анализе сайтов, данные с которых попали в интернет, специалисты Group IB выяснили, что на некоторых ресурсах файл robots.txt был вообще не заполнен. "Администраторы этих сайтов не предпринимали никаких действий по ограничению доступа к веб-страницам", - отмечает Никитин.

Генеральный директор компании "1С-Битрикс" (разработчик программного обеспечения для создания сайтов) Сергей Рыжиков уверен, что последние инциденты - яркий пример безалаберности разработчиков и отсутствия внимания к теме безопасности. Рыжиков отмечает, что зачастую защита персональных данных пользователей на ресурсе остается за пределами бюджета проекта. "На нее не выделяют деньги ни заказчики, ни веб-разработчики. Не удивительно, что о проблемах узнают даже автоматизированные системы, такие, как поиск "Яндекса", не говоря уже о злоумышленниках", - отмечает Рыжиков.

Разработчик софта для интернет-магазинов, компания WebAsyst, под давлением фактов (пострадали персональные данные покупателей именно тех магазинов, которые использовали программный продукт Shop-Script разработки WebAsyst) вынуждена была признать ответственность за инцидент.

"Яндекс" призывает разработчиков сайтов внимательно изучить инструкции по корректному использованию

файла robots.txt и исполнять их.

Признаков надежности нет

Эксперты отмечают, что сейчас в рунете невозможно отличить надежный сайт, данные на котором будут защищены, от сайта, на котором пользователь рискует потерять персональные данные.

"Не существует общего правила для пользователей по выявлению таких неблагонадежных ресурсов. Однако в первую очередь им стоит обращать внимание на то, каким образом осуществляется авторизация и доступ к данным", - отмечает Никитин. Если на сайте применена парольная защита, и доступ происходит с использованием защищенного протокола SSL, то ресурс, скорее всего, надежен. Также нужно уточнить, использует ли сайт cookies (файлы со служебными данными, хранимыми сайтом на диске пользователя). Cookies позволяют "привязать" конкретного пользователя к определенной веб-странице, исключив доступ к ней поисковым роботам.

Рыжиков уверен, что России не помешала бы сертификация интернет-магазинов: "В Европе существует ассоциация Trusted Shops, среди ее задач - проверка и сертификация интернет-магазинов, после чего они получают разрешение разместить на своих страницах специальный знак", - отмечает он.

Ответят владельцы магазинов

Сведения о заказах, которые попали в открытый доступ со страниц интернет-магазинов, относятся к категории персональных данных. По словам заместителя генерального директора по правовым вопросам компании Group-IB Сергея Грудинова, обязанность обеспечивать конфиденциальность персональных данных, т.е. не допускать их распространения без согласия клиентов и принимать необходимые организационные и технические меры для защиты данных от неправомерного или случайного доступа к ним, лежит в конкретном случае на интернет-магазинах - они выступают в роли операторов персональных данных.

Однако Грудинов отмечает, что ответственность за распространение данных клиентов интернет-магазинов могут понести сразу несколько сторон. "Если подобная "утечка" произошла вследствие полного игнорирования владельцами интернет-магазина норм законодательства по защите персональных данных - вина целиком и полностью на них", - говорит он.

Вина ляжет на руководство ресурса и в том случае, если утечка связана с некорректной настройкой техническими сотрудниками магазина аппаратно-программной части, из-за чего и произошел сбой в системе безопасности.

"С другой стороны, проблема может заключаться именно в программном комплексе, имеющем не декларированные в сопроводительной документации возможности. Тут, конечно, непосредственно интернет-магазин ни при чем, а все вопросы могут быть адресованы к разработчику данного ПО", - отмечает Грудинов.

Хакеров никто не отменял

Несмотря на то, что инциденты с публикацией данных в поисковой выдаче стали предметом многочисленных обсуждений, пользователям стоит опасаться не этого, говорят эксперты.

"Последние инциденты с поисковыми системами, которые мы наблюдаем, не идут не в какое сравнение с целенаправленными действиями хакеров, которые получают куда больше пользовательских данных при совершении атак на интернет-сайты. Разница лишь в том, что хакер хочет извлечь выгоду, а не продемонстрировать уязвимость, поэтому полученные данные после проведения атаки обычно не попадают в свободный доступ", - считает ведущий эксперт Positive Technologies Дмитрий Евтеев.

Автор: Артур Скальский © Digit ИНТЕРНЕТ И ИТ, МИР 2917 27.07.2011, 13:38 535
URL: https://babr24.com/?ADE=95505 Bytes: 6743 / 6707 Версия для печати Скачать PDF

- ВКонтакте

Связаться с редакцией Бабра:
newsbabr@gmail.com

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта