Взломы баз данных

Взлом базы данных представляет собой неправомерное использование информационной системы. Это серьезное преступление. Случаи, когда преступники завладевают персональными данными, вызывают серьезную обеспокоенность. На этом сайте мы собрали общую информацию об утечках данных и советы о том, что делать, если вы подозреваете, что стали жертвой утечки данных. Здесь же вы найдете и ответы на часто задаваемые вопросы. Следите за информацией о происшествии по надежным источникам. Не следует забывать, что не вся информация, которая публикуется в социальных сетях, является достоверной. Не распространяйте слухи и не делитесь своими персональными данными.

Где получать информацию?

1

Информация о взломе базы данных муниципалитета Хельсинки

- На сайте муниципалитета Хельсинки по адресу **hel.fi/tietomurto** вы найдете дополнительную информацию о случившемся.
- Муниципалитет Хельсинки, служба по работе с клиентами, ставшими жертвами утечки персональных данных: пн.–пт. 8.00–18.00, тел. 09 310 27139 или **kaskotietoturvatilanne@hel.fi**
- Кризисная служба муниципалитета Хельсинки: пн.-вс круглосуточно, тел. 09 310 44222.

2

Помощь по вопросам утечки персональных данных на сайте Suomi.fi

Рекомендации органов власти для лиц, пострадавших от утечки данных, в сервисе Suomi.fi і **https://www.suomi.fi/oppaat/tietovuoto**

В этом руководстве рассказывается о том, что следует предпринять, чтобы ваши персональные данные не оказались в руках злоумышленников. Руководство содержит рекомендации для пострадавших от взлома информационной системы и утечки данных, и предоставит вам помощь, если ваши персональные данные были похищены, или вы потеряли документы, например, паспорт или удостоверение личности.

3

Куда можно позвонить, если вы волнуетесь из-за утечки персональных данных:

Кризисная служба муниципалитета Хельсинки: пн.-вс. круглосуточно, тел. 09 310 44222

Кризисный телефон организации MIELI ry, пн.-вс. круглосуточно, тел. 09 2525 0111

Часто задаваемые вопросы о взломе базы данных и утечке персональной информации

Что такое – взлом базы данных?

Взлом базы данных представляет собой неправомерное проникновение в информационную систему, сервис, устройство или приложение, например, несанкционированное пользование аккаунтом электронной почты при помощи полученных в распоряжение идентификаторов (имени пользователя и пароля). Взлом базы данных является наказуемым деянием, предусмотренным уголовным кодексом. Попытка взлома базы данных также наказуется. Само по себе несанкционированное проникновение в систему является преступлением, и для его квалификации как преступления не требуется даже факта использования информации, которая находилась на объекте взлома или использовалась на нем.

С какой целью и кто взламывает базы данных?

Мотивы взломов баз данных трудно установить. Часто их целью является получение финансовой выгоды. Например, финансовую ценность представляют защищенные данные, находящиеся в системе. Взломанная информационная среда также может быть использована для распространения вредоносных материалов или выведена из строя с помощью программ-вымогателей. Злоумышленник может использовать взломанную среду и для других атак, например, для атак типа «отказ в обслуживании» (DoS).

Преступник может иметь умысел на причинение вреда, шантаж и даже шпионаж в пользу какого-либо государства. Базы данных взламывают преступники, лица, находящиеся на службе у государства, и даже частные лица. Взломы баз данных происходят постоянно, но серьезные инциденты случаются не очень часто.

Сколько попыток взлома баз данных предпринимается и выявляется в Финляндии ежегодно?

Ежегодно выявляется значительное количество взломов баз данных. Однако большинство из них довольно безобидны. Это, например, взломы аккаунтов в социальных сетях или кража банковских паролей при интернет-мошенничестве (фишинг).

Какие изменения претерпели взломы баз данных за последние годы?

Самое значительное изменение во взломе баз данных заключается в том, что злоумышленники научились добывать коды многофакторной аутентификации, которые используются для входа в системы. Благодаря использованию

искусственного интеллекта улучшилось языковое сопровождение фишинговых кампаний.

Как можно использовать похищенные данные?

Похищенные данные могут быть опубликованы без разрешения их владельца, или завладевшее такими данными лицо может шантажировать жертву, требуя выкуп. Данные могут использоваться в преступных целях для причинения вреда, вымогательства или шпионажа.

Взломы баз с данными частных лиц могут использоваться, например, для кражи персональных данных, когда другое лицо пытается выдать себя за того, чьи персональные данные были похищены при взломе. Взломы информационных систем могут производиться и просто с целью преследования. Если человек становится жертвой утечки данных, у него могут возникать сбои при использовании компьютерных систем. Также он может пострадать от последствий попадания его персональных данных в чужие руки.

Как можно защититься от утечки персональных данных?

Для частного лица самый эффективный способ защиты – использование многофакторной аутентификации и общие представления о компьютерной безопасности. Под многофакторной аутентификацией понимается использование дополнительного средства идентификации пользователя помимо имени пользователя и пароля. Примером дополнительных средств идентификации могут служить списки одноразовых цифровых ключей, как в онлайн-банках, и коды, отправляемые на мобильный телефон. В таком случае злоумышленнику, завладевшему именем пользователя и паролем жертвы, при использовании многофакторной аутентификации необходимо получить еще и одноразовый код для входа в информационную базу и хищения данных.

Случаи, когда преступники завладевают персональными данными, вызывают серьезную обеспокоенность. Можно стать жертвой утечки персональных данных, даже если делать все правильно.

Руководство по защите от утечки данных для частных лиц, разработанное Центром кибербезопасности (Ссылка на сторонний ресурс)

Руководство по защите от утечки данных для организаций, разработанное Центром кибербезопасности (Ссылка на сторонний ресурс)

Чем занимается Центр кибербезопасности Traficom, в чем заключается его роль?

Задачей службы CERT Центра кибербезопасности, то есть ситуационного центра, является предотвращение и расследование угроз информационной безопасности, а

также предоставление информации по вопросам безопасности данных. Служба CERT обрабатывает сообщения об угрозах информационной безопасности и оказывает обратившимся с такими сообщениями организациям помощь в устранении угроз. Центр кибербезопасности также информирует общественность и разрабатывает рекомендации о том, что делать частным лицам, если их персональные данные стали объектом взлома или утечки.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Информация о взломе базы данных муниципалитета Хельсинки (Ссылка на сторонний ресурс)
Информационное сообщение управления полиции Хельсинки: Полиция расследует масштабную утечку данных из компьютерной сети муниципалитета Хельсинки (Ссылка на сторонний ресурс)
Руководство «Утечка данных» Tietovuoto.fi (Ссылка на сторонний ресурс)
Офис уполномоченного по защите информации (Ссылка на сторонний ресурс)
Новость на сайте Центра кибербезопасности: Взломы баз данных – что это такое?
Инструкция, разработанная Центром кибербезопасности: Как защититься от утечки данных
Редакция от 13.05.2024