

pressrelease

Gemalto опубликовала Индекс критичности утечек данных за 2016 год

В 2016 году было скомпрометировано почти 1,4 млрд. записей данных, что обусловлено атаками злоумышленников на крупные предприятия различных отраслей

Амстердам, 28 марта 2017 года – Компания Gemalto (Euronext NL0000400653 GTO), мировой лидер в области технологий цифровой безопасности, сегодня опубликовала результаты Индекса критичности утечек данных ([Breach Level Index](#)), согласно которым в 2016 году в мире было зафиксировано 1792 инцидента, которые привели к компрометации 1,4 миллиарда записей данных, что на 86% выше по сравнению с 2015 годом. Кроме того, отмечается, что хищение персональных данных стало наиболее распространённым видом утечек. В 2016 году – на долю таких атак приходилось 59% всех зафиксированных инцидентов. Кроме того, в 52% случаев при публикации информации об утечке в 2016 году компании не сообщали о количестве скомпрометированных записей.

Индекс критичности утечек данных представляет собой глобальную базу утечек и обеспечивает оценку уровня той или иной утечки данных по различным параметрам, в том числе по типу данных и количеству похищенных записей, источнику утечки, характеру использования похищенных данных, а также по тому, были ли украденные данные зашифрованы. Каждая утечка получает определенный балл, таким образом, индекс критичности утечек данных представляет собой сравнительную таблицу утечек, позволяющую отличить мелкие и незначительные инциденты от действительно крупных и значимых утечек (балл утечки варьируется от 1 до 10). Согласно Индексу критичности утечек данных, за период с начала составления индекса публично зафиксированных утечек в 2013 году, количество скомпрометированных записей данных превысило 7 миллиардов. Таким образом, в среднем в мире ежедневно компрометируется более 3 миллионов записей данных, или, грубо говоря, 44 записи каждую секунду.

В прошлом году в результате атаки на базу учётных данных пользователей AdultFriend Finder было скомпрометировано 400 миллионов записей, а сам инцидент получил максимальный балл (10) в Индексе критичности утечек. Среди других крупных утечек, зафиксированных в 2016 году, – атака на Fling (BLI: 9,8), утечка в избирательной комиссии на Филиппинах (COMELEC) (BLI: 9,8), 17 Media (BLI: 9,7) и Dailymotion (BLI: 9,6). Фактически, на долю 10 самых крупных и масштабных утечек пришлось более половины всех скомпрометированных записей данных. В 2016 году интернет-гигант Yahoo! сообщил о двух крупных утечках, в результате которых было скомпрометировано 1,5 миллиарда учётных записей пользователей, но эти утечки не вошли в индекс BLI за 2016 год, поскольку инциденты датировались 2013 и 2014 годом.

В России среди всех утечек данных, можно выделить несколько наиболее значимых. Самой крупной среди них является атака на базу учетных данных Mail.ru (BLI: 9,0), в ходе которой было скомпрометировано более 25 миллионов записей. Данные включали в себя имена пользователей, email-адреса, зашифрованные пароли и даты рождения, в некоторых случаях злоумышленникам также удалось узнать IP-адреса пользователей и их телефонные номера. Среди других утечек, зафиксированных в 2016 году на территории РФ – атака на мультипортал KM.ru (BLI: 8,1) и компанию по разработке программного обеспечения Nival (BLI: 8,1). Доля похищенных данных в обоих случаях составляет более 1,5 миллиона учетных записей.

pressrelease

"Индекс критичности утечек данных свидетельствует о четырёх основных тенденциях, которые наблюдаются в мире киберпреступности в последние годы. Злоумышленники расставляют всё больше сетей и используют легко добываемые учётные и персональные данные в качестве отправной точки для достижения более сложных и многообещающих целей. Очевидно, что злоумышленники также переориентируются с атак, нацеленных на финансовые организации, на проникновение в крупные базы данных – например, развлекательных сайтов или социальных сетей. Наконец, нередко они с помощью шифрования делают данные на атакованных устройствах нечитаемыми, а затем требуют выкуп, – говорит Джейсон Харт (Jason Hart), вице-президент и директор по технологиям в подразделении защиты данных в Gemalto.

Утечки данных по типу

В 2016 году наиболее распространённым видом инцидентов стало хищение персональных данных – на долю таких атак приходилось 59% всех утечек данных, что на 5% выше, чем в 2015 году. Вторым по распространённости типом утечек данных в 2016 году стали утечки учётных записей пользователей. Хотя число утечек такого типа сократилось на 3%, на их долю приходилось 54% всех скомпрометированных записей, что на 336% выше по сравнению с прошлым годом. Это свидетельствует о новой тенденции, когда злоумышленники переориентируются с атак с целью получения финансовой информации на атаки на крупные базы данных с большими объёмами идентификационных и персональных данных. Ещё одним распространённым типом инцидентов стала категория незначительных атак (nuisance category), число инцидентов в которой увеличилось на 102%, но на долю которых приходится 18% от всех скомпрометированных записей данных, что на 1474% выше по сравнению с 2015 годом.

Утечки данных по источнику

Наибольшее число утечек было организовано злоумышленниками, действующими извне организаций – на долю таких атак приходилось 68% всех инцидентов, что на 13% выше, чем в 2015 году. Количество скомпрометированных записей данных в результате действий сторонних злоумышленников увеличилось на 286% по сравнению с 2015 годом. Количество утечек данных, организованных хакерами-активистами, также увеличилось в 2016 году – на 31%, но на их долю приходится лишь 3% всех зафиксированных в прошлом году инцидентов.

Утечки данных по отрасли

В разбивке по отраслям наибольший рост числа утечек в 2016 году пришелся на технологический сектор. Количество инцидентов выросло на 55%, но тем не менее на их долю приходилось лишь 11% всех утечек за минувший год. Почти 80% всех инцидентов в этом секторе связаны с хищением учётных записей и персональных данных. Кроме того, на их долю приходится 28% всех скомпрометированных записей данных в 2016 году, что на 278% выше, чем в 2015 году.

На предприятия отрасли здравоохранения пришлось 28% всех утечек данных, что на 11% выше, чем в 2015 году. Однако количество скомпрометированных записей данных в этой отрасли снизилось на 75% по сравнению с 2015 годом. В секторе образования количество утечек данных за год снизилось на 5%, а количество скомпрометированных записей данных упало на 78%. На долю государственных учреждений приходилось 15% всех утечек данных в 2016 году. Однако количество скомпрометированных записей данных выросло на 27% по

pressrelease

сравнению с 2015 годом. На долю компаний финансового сектора приходилось 12% всех утечек данных, что на 23% ниже по сравнению с прошлым годом.

На долю других отраслей приходилось 13% всех утечек данных и 36% скомпрометированных записей данных. В этой категории общее количество утечек данных снизилось на 29%, однако количество скомпрометированных записей выросло на целых 300% по сравнению с 2015 годом. При этом большинство утечек данных приходилось на социальные сети и сайты компаний из отрасли развлечений.

В прошлом году количество инцидентов, затрагивающих полностью или частично зашифрованные данные, составляло 4,2% от общего числа инцидентов, тогда как в 2015 году эта цифра составляла лишь 4%. В части этих утечек зашифрованным был только пароль, а остальная информация не была зашифрована. Однако из почти 1,4 миллиарда скомпрометированных, утраченных или похищенных записей данных в 2016 году полностью или частично зашифровано было лишь 6% (в сравнении с 2% в 2015 году).

"Точное понимание того, где именно размещаются корпоративные данные и кто именно имеет к ним доступ, позволит предприятиям лучше сформулировать свои стратегии безопасности, с учётом тех видов данных, которые являются наиболее важными для них. Шифрование и аутентификация уже не просто некие "передовые практики", а самая настоящая необходимость. Это особенно справедливо с принятием новых и обновлением уже существующих государственных стандартов, в том числе с грядущим принятием общего законодательства в отношении защиты данных (General Data Protection Regulation, GDPR) в Европе, а также с принятием внутриштатного (в США) и общенационального (в Азиатско-тихоокеанском регионе) законодательства о публикации информации об утечках. Кроме того, речь идёт о защите целостности данных вашего бизнеса, поэтому от правильности решений зависит ваша репутация и прибыль".

Дополнительная информация:

- Для получения полной сводки всех утечек данных с разбивкой по отраслям, источникам, типу и географии, загрузите [Индекс критичности утечек данных за 2016 год](#) или получите доступ к eBook по [ссылке](#).
- Скачать инфографику вы можете по [ссылке](#).
- Посетить сайт Индекса критичности утечки данных вы можете по [ссылке](#).

О компании Gemalto

Компания Gemalto является мировым лидером в сфере [цифровой безопасности](#) с клиентами более чем в 180 странах и годовым доходом в 3,1 млрд евро.

Наши технологии и сервисы позволяют компаниям и государственным органам, подтверждая подлинность учетных записей и защищая их персональные данные, обеспечивать надежную безопасность пользователей. Также они предоставляют возможность использования защищенных сервисов как на персональных устройствах, подключенных к сети предметам и в облаке, так и для осуществления безопасной передачи данных между ними.



pressrelease

Решения Gemalto находят широкое применение в современной жизни, начиная с платежных операций и систем, заканчивая инфраструктурой корпоративной безопасности и Интернетом вещей. Мы осуществляем аутентификацию пользователей, транзакций и объектов, выполняем шифрование данных и создаём дополнительные преимущества и ценность для программных продуктов, позволяя нашим клиентам предлагать защищенные цифровые сервисы для миллиардов пользователей и объектов.

Штат компании насчитывает более 14 тысяч сотрудников, которые работают в 118 офисах, 45 центрах персонализации и обработки данных, 28 центрах исследований и программирования, расположенных в 52 странах мира.

Дополнительная информация представлена на сайте www.gemalto.com или следите за сообщениями [@gemalto](https://twitter.com/gemalto) в Twitter.

Контакты для прессы Gemalto:

Алексей Мальцев

+7 (963) 617-24-78

Иван Фролов

+7 (963) 641-15-28

Gemalto@grayling.com