УДК 004.62

ВСКРЫТИЕ ПАРОЛЯ

Хамзина Э.И., студентка 3 курса экономического факультета
Научный руководитель – Голубев С.В, к.э.н., доцент
ФГБОУ ВО Ульяновский ГАУ

Ключевые слова:*криптоанализ, вскрытие пароля, киберпреступления, администратор, пользователи, информация.*

Работа посвящена актуальной в наше время проблеме развития киберпреступности, а именно вскрытия паролей в сети.

В сферах криптоанализаикомпьютерной безопасности,вскрытие пароляпредставляет собой процедуру восстановленияпаролейиз данных, которые были сохранены или переданы с помощью компьютерной системы. Общий подход состоит в том, чтобы подбором угадать пароль. Другим известным методом является «забытие» пароля, чтобы потом изменить его.

Целью взлома пароля может являться помощь пользователю в восстановлении забытого пароля, получение незаконного доступа к системе, или же профилактическая мера, когда системные администраторы хотят проверить насколько легко взламываются пароли.

Люди часто пользуются легко запоминающимися паролями, которые прямо или косвенно имеют отношение к их личной жизни: именаблизких, кличка питомца, дата рожденияи т.п. Но злоумышленнику достаточно взглянуть нарабочий стол человека, чтобы получить представление о возможных вариантах его пароля. Вот почему хороший пароль нужно составлять из набора букв нижнего и верхнего регистров, цифр и специальных символов.

Более миллиона людей каждый день становятся жертвами киберпреступников, а каждый час в мире совершается более 50 000 взломов, атак и других преступлений.Если говорить о причинах взлома, то, согласно статистике, в 20% случаев это были «дыры» в системе безопасности, 12% – результат заражения компьютера, 6% опрошенных указали на кражу пароля от сайта. 2% участников опросов предположили, что кража – результат входа на сайт через компьютер публичного пользования или беспроводную сеть.

Чтобы максимально обезопасить себя от взлома паролей необходимо следовать нескольким правилам:

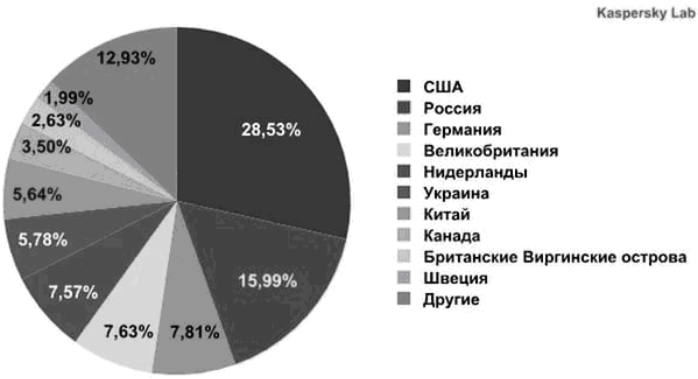

Рисунок 1 - Статистика стран с наибольшим уровнем киберпреступности

- Придумать наиболее сложные пароли.
- Установить время «жизни» паролей и регулярно их менять.
- Обеспечить неразглашение паролей.
- Не оставлять без присмотра работающие терминалы и серверы.
- Поддерживать политику учетных записей и регулярно пересматривать параметры этих записей.
- Ограничить численность администраторской группы.
- Указать пользователям сети на то, что в случае обнаружения проблемы они должны обязательно обратиться к администратору.

Пароли должны иметь свое время «жизни». Чем дольше используется пароль, тем больше вероятность его раскрытия или разглашения. Администраторский пароль должен меняться чаще других.

Пересмотр параметров учетных записей позволяет вовремя определить, нужен ли пользователю доступ к тому или иному ресурсу. Периодичный проверкаучетных записей пользователей (особенно анонимных пользователей) нужен главным образом потому, что появляются новые каталоги внутри старых ресурсов и таким образом пользователи автоматически имеют доступ к этим каталогам. Для слежения за изменениями учетных записей существуют различные средства аудита, которые встроены в ОС.

Пользователи должны знать, что при обнаружении проблем, которыемогут быть связаны с безопасностью, они могут обратиться к

администратору. Во многих случаях пользователи первыми обнаруживают ошибкив работе систем, до того, как это становится известным администратору. При этом обнаруживший ошибку не спешит обращаться к администратору, боясь, что его обвинят во взломе сайта. А если об этом будет вовремя доложено администратору, он сможетзакрывать бреши до того, как они будут обнаружены злоумышленником.

Также необходимо изменять установленный по умолчанию пароль,в частности, администраторские паролиWeb-сервера, которыемогут быть использованы для доступа к системе хакером.

Существует разнообразные средства вскрытия парольной защиты, которые могут быстро взламывать закрытые документы, а также пароли, используемые в сети. Например, программа DistrubutedPassw ordRecoveryпозволяет мгновенно, вскрывать зашифрованные пароли и документы, хранящиеся в сети. В случае использования в корпоративной среде такая система позволяет однозначно определить степень стойкости политики шифрования, которая применяется на вашем предприятии. Еще одна программа -ElcomsoftPasswordRecoveryBundle предоставляет менеджерам, администраторам по поддержке в области информационных технологий и правоохранительным органам получить доступ к различным защищенным паролями документам, которые были случайно или намеренно защищены паролями.

Киберпреступность приобрела глобальные масштабы, и эта проблема стремительно нарастает. Правоохранительные органы принимают меры борьбы с ней - законодатели принимают новые законы, полицейские агентства формируют специальные подразделения по борьбе с киберпреступностью. Однако проблема является слишком большой и широко распространенной, чтобы с ней можно было быстро и легко справиться.

Библиографический список

1. Куликова, А.И. Компьютерная преступность в современном обществе / А.И. Куликова, В.В. Васильченко.- М.: ЮНИТИ, 2015.- 120 с.
2. Компании терпят убытки от простых паролей пользователей // Экономическая безопасность предприятия. - 2016. - N 1. - С. 24-26.
3. Как взламывают «операционную систему» человека // Экономическая безопасность предприятия. - 2015. - N 2. - С. 33-38 .
4. Добрикова, Е. Персональные данные: успеть обеспечить защиту / Е. Добрикова // Экономическая безопасность предприятия. - 2015. - № 1.- С. 81-87.

OPENING PASSWORD

Khamzina E.I.

Key words: *cryptanalysis, break passwords, cybercrime, administrator, users, information.*

The work is devoted to a topical problem of development of cybercrime, namely opening the passwords in the network.