Рекомендации по парольной защите

Поработав с ПО от компании Elcomsoft, понял, что рекомендации по парольной защите нуждаются в существенных дополнениях и обновлениях Отсюда и родилась данная статья.

Парольная аутентификация в Windows

1. Длина пароля не менее 15 символов для обычного пользователя и 20 для администратора.
2. В пароле должно быть не менее 3 наборов символов из 4-х
3. Каждая учетная запись (почта, ПК, домашняя почта, сайты в интернет) должны иметь не повторяющиеся пароли
4. Пароль ни в коем случае не должен быть словарным словом.

К чему это приведет? Пользователь сегодня должен помнить минимум 8-10 паролей. Вывод напрашивается уже давно. ***Необходимо использовать многофакторную аутентификацию.***

Дорого? Да! А что делать? Не знаю!

Парольная защита документов Office

В связи с тем, что в документах Office 2007/2010 реализовано шифрование по алгоритму AES с длиной ключа 128 символов, рекомендуется документы шифровать именно в формате docx. Хотелось бы отметить, что пароли в файлах, созданных в формате Office 2010 перебираются медленнее чем в Office 2007. Средняя скорость перебора – 200 паролей в секунду (без применения технологий подбора паролей с помощью ресурсов видеокарт). Следовательно – длина пароля не менее 10 символов и формат Office 2010.

Парольная защита архивов

Наиболее часто употребляемые форматы архивов (на мой взгляд) – .zip, .rar. В архиваторе WinZip реализовано три алгоритма шифрования:

1. Standard Zip 2.0 encryption – используется по умолчанию.
2. 128-bit AES encryption – криптографический алгоритм AES с длиной ключа 128 бит.
3. 256-bit AES encryption – криптографический алгоритм AES с длиной ключа 256 бит (усиленный алгоритм шифрования).

Выбираем шифрование с помощью 128-bit AES encryption (256-bit AES encryption) при условии, что распаковываем с помощью WinZip.

В архиваторе WinRAR используется алгоритм шифрования AES с длиной ключа 128 бит. Стоит отметить, что файлы, зашифрованные в WinRAR, будут открываться и в WinZip. Однако обратное будет работать лишь для алгоритма шифрования Zip 2.0.

К недостаткам шифрования WinZip стоит также отнести то, что WinZip не шифрует комментарии zip-файлов и такие свойства зашифрованных файлов как наименования, даты и т.д. А ведь это весьма ценная информация для аналитика. Ведь далеко не всякий пользователь переименовывает архивируемые файлы, а уж тем более изменяет остальные атрибуты (дата создания, изменения, размер и т.д.). Длина пароля не менее 10 символов. Пароль содержит 3 набора символов из 4-х.

Пароли к сайтам

Ни в коем случае не сохранять пароли к сайтам в браузерах!

Пароль к Windows Live

Ни в коем случае не сохранять! Пароль хранится в реестре и легко извлекается оттуда

Заключение

Надеюсь эти не сложные рекомендации помогут вам.