# Слабое звено, или Layer 8 в модели OSI

**Сергей ТРОИЦКИЙ,**
**преподаватель учебного центра «Информзащита»**

Есть известная шутка, что в канонической системной 7-уровневой модели OSI наиболее уязвим восьмой – пользователь на консоли системы. Но при обсуждении проблем безопасности ИКТ систем довольно часто можно встретить игнорирование наличия в этой системе человека. Особенно часто к такому восприятию склоняются инженеры, системные администраторы и программисты. Хотя и в среде обычных пользователей часто наблюдаются следы похожего подхода, правда, в немного другом виде: «технологии настолько сложны, что сродни магии, потому человеку остается только бояться, исполнять предписанные ритуалы и уповать на цифрового бога». Однако часто простые и человечные методы (никакой математики, только здравый смысл) оказываются эффективнее сложных технических решений.

Как же влияет Layer 8 на безопасность в цифровом мире?

Немного статистики

По традиции в новом году подводятся итоги прошлого. Этой традиции последовали и компании, занимающиеся вопросами кибербезопасности. Компании IBM и Symantec, например, выпустили отчеты по состоянию цифровой безопасности за 2017 г. Общий вывод таков: пользователи сильно переоценивают свой уровень подготовленности в вопросах цифровой безопасности, что сделало их уязвимыми к атакам и дало возможность киберпреступникам достичь в прошедшем году рекордной эффективности. При этом разные поколения пользователей делают упор на разных средствах обеспечения безопасности.

Прошедший год, по статистике Symantec, стал рекордным по количеству пострадавших от киберпреступлений. Основные статистические показатели этого своеобразного «рекорда» таковы:

- 978 млн пострадавших в 20 странах мира за год.
- 44% из всех пользователей сети интернет подвергались за прошедший год атакам того или иного сорта.

С какими видами преступлений чаще всего сталкивались люди в сети:

- Заражение устройства компьютерным вирусом или другим зловредным ПО (53%).
- Мошенничество с платежными картами (38%).
- Кража пароля учетной записи (34%).
- Несанкционированный доступ или взлом ящика электронной почты или учетной записи социальной сети (34%).
- Онлайн-покупка, завершившаяся потерей денег через мошенничество (33%).
- Реакция на поддельное сообщение электронной почты – предоставление в ответ на такое сообщение своих персональных (личных или финансовых) данных мошенникам (32%).

Суммарные потери от киберпреступности в прошлом году оценены компанией Symantec в $172 млрд – в среднем по $142 на пострадавшего. Общие потери времени на устранение последствий потребовало 24 часов (три полных рабочих дня) времени в глобальном масштабе.


**Суммарные потери от киберпреступности в 2017 году**
По оценкам компании Symantec

**Возраст имеет значение?**

Кто же он, средний пострадавший от киберпреступности прошлого года? Есть ли какое-то поколение, иммунное к уловкам мошенников новой эпохи? Оказывается, «любви все возрасты покорны», хотя и все по-разному. От «бэби-бумеров»[1] до «детей нулевых», все поколения по-своему «забывали закрывать цифровую дверь».

Молодое поколение оказалось наиболее продвинутым технологически. У них самое большое количество различных цифровых устройств (в среднем по 4 на душу), и именно они наиболее охотно используют самые продвинутые техники защиты (32%) – распознавание лиц, VPN, поведенческий анализ, голосовую и двухфакторную идентификацию. Однако при этом именно они чаще совершают элементарные ошибки: например, применяют плохую парольную политику (70%). В итоге миллениалы дали 60% жертв киберпреступлений по миру за прошлый год.

Каждый четвертый (26%) в этой возрастной группе использует один пароль для всех своих учетных записей. Из старших поколений такую практику применяли только 10% пострадавших. 63% пострадавших из молодого поколения, по

**Торгово-транспортная компания «Концепт»**

Доставка грузов
Китай- Казахстан- Россия

КИТАЙ
КАЗАХСТАН
РОССИЯ

Телефоны: **8 -499-369-50-52**
**8-499-369-01-35**
Почта: **china-koncept@mail.ru**
Сайт: **www.china-koncept.ru**
Офисы: **Москва, Алматы**

[1] Рожденные в период с 1940 по 1960–1964 гг. (https://en.wikipedia.org/wiki/Baby_boomers)

крайней мере, один раз делились доступом к своим учетным записям с другими (в старших поколениях таких было 36%).

Старшие поколения оказались более осторожными, хотя и тут не обошлось без проколов:

- 61% «отцов и матерей» и 2/3 «бабушек и дедушек» использовали разные пароли для разных сервисов, но 39% первых и 49% вторых при этом записали их на бумажку (увы, память не становится лучше с годами).
- Старшее поколение в мировом масштабе пренебрегает резервным копированием, 16% вообще не осуществляли резервного копирования ни одного из своих устройств.
- Показательно, что среднее поколение потеряло больше остальных возрастных групп – $167 в среднем – на 15% выше общего среднего значения по миру.

Родители очень беспокоятся о своих детях, когда речь идет об интернете, но при этом мало что делают. 96% родителей вопрос безопасности детей в интернете тревожит, но только треть отслеживает, в какие онлайн-игры играют их отпрыски и что они там делают, в каких соцсетях общаются и какие сайты посещают. А 11% при этом не предпринимают вообще никаких действий для защиты своих детей в онлайне.

**Грань между реальностью и виртуальностью**

По статистике Symantec, подавляющее большинство опрошенных (81%) полагают, что за киберпреступления надо наказывать как за обычные. Но в то же время 43% пользователей полагает приемлемым в определенных условиях совершать в онлайне действия, сомнительные с моральной точки зрения. Например, более четверти опрошенных считают, что можно читать чужую электронную почту, 21% полагают, что пользоваться чужим почтовым адресом для идентификации приемлемо. 15% даже считают приемлемым получать доступ к чужим финансовым онлайн-инструментам без разрешения владельца.

Показательно, что более половины пострадавших от киберпреступности имеют сниженную планку морали в отношении онлайн-общения (в два раза чаще они оправдывают чтение чужой почты, в полтора раза чаще склонны выдать себя за другого человека в онлайне и примерно настолько же более склонны к более вольному обращению с чужими онлайн-финансами).

**«Верить нельзя никому. Мне – можно» (старина Мюллер)**

Доверчивость людей, однако, не подорвана массовым выходом в онлайн и столкновением с киберпреступностью. Доверить свои персональные данные и личную информацию сторонним агентам люди все еще готовы: 76% верят органам по защите персональных данных, 80% – интернет-провайдерам и провайдерам услуг электронной почты, 82% – финансовым организациям. Что интересно, собственным правительствам верят гораздо меньше – таких только 41% от опрошенных пользователей.

**Врачу – да исцелися сам**

Были ли ИТ-специалисты менее склонны к небезопасному поведению и практикам? Как показывают масштабы заражения корпоративных сетей вирусами WannaCry, Petya, ExPetya, NotPetya, административный и технический персонал корпораций часто пренебрегал простыми мерами безопасности, основанными на здравом смысле и организационных мерах, в пользу высокотехнологичных, но без должной настройки и мониторинга малоэффективных средств.

Довольно большое количество зараженных WannaCry промышленных компьютеров объясняется, по мнению специалистов «Лаборатории Касперского», небезопасными практиками сетевых специалистов при конфигурации сетевых сегментов. Среди причин распространения вируса в корпоративных и технологических сетях перечислены создание мостов между технологическим (без доступа в интернет) и общим сегментами корпоративной сети (для удобства администрирования), разрешение удаленного доступа к технологической сети из сегмента DMZ, пренебрежение рекомендациями вендоров ПО по установке исправлений и безопасной настройке компонентов. Масштабы заражений показывают, сколько администраторов пренебрегли простым здравым смыслом и не внедрили у себя минималистского подхода к настройке серверов и рабочих станций. Простое отключение ненужных сервисов, сегментация сети, аудит системных учетных записей и их прав (например, снятие привилегии debug с группы встроенных администраторов в случае с WannaCry) могли бы сильно затруднить, если не предотвратить масштабные эпидемии прошлого года.

**Что делать?**

Что же рекомендуют специалисты компаний IBM и Symantec? Простые методы, диктуемые здравым смыслом, более эффективны в деле защиты от угроз цифровой эпохи.

Пароли: создать (и запомнить!) несколько хороших паролей часто оказывается лучше увлечения высокотехнологическими средствами (биометрия, двухфакторная аутентификация и т. п.). Не стоит создавать пароль на основе общедоступных личных данных. Хорошо сделать пароль длинным, но при этом легко запоминающимся. Также не стоит пренебрегать и новыми технологиями – двухфакторная аутентификация, биометрическая защита и менеджеры паролей способны заметно снизить уязвимость личных данных.

Сети: важно четко понимать, что работа через незащищенную WiFi сеть сопряжена с высокой вероятностью перехвата ваших данных (финансовых, личных и др.). Возможно, в этом случае стоит рассмотреть варианты с VPN доступом к ценным личным ресурсам.

Устройства: подключая новое устройство к своей сети, полезно убедиться в надежности защиты – сменен ли пароль по умолчанию на встроенной учетной записи, выключены ли ненужные вам сервисы. Также если устройства беспроводные, убедитесь в достаточной надежности вашего пароля WiFi (тот случай, когда именно длина, а не сложность имеет большее значение) и отсутствии проблем с безопасностью в прошивке вашей точки доступа.

Поведение: не поддавайтесь искушению расслабиться, общаясь в соцсетях или читая электронную почту. Фишинг становится все более распространенным и более интеллектуальным и персонализированным, поэтому не стоит переоценивать свою внимательность. Тщательно проверьте источник письма, тип прицепленного файла, убедитесь в достоверности ссылки, прежде чем запустить что-либо. Антивирусные программы полезны, но не всесильны, потому, даже имея актуальное защитное ПО, расслабляться не стоит.

Управление: администраторы и технический персонал тоже люди, им свойственно то же стремление к удобству и комфорту. Отсюда применение небезопасных сетевых конфигураций, пренебрежение рекомендациями вендоров ПО по настройке и установке исправлений, избегание документирования операций и т. д. Но и тут здравый смысл и прозрачные и четкие организационные меры заметно эффективнее высокотехнологичных решений. А самым лучшим вариантом будет сочетание простых базовых методов с серьезными технологиями защиты и ясными процедурами настройки и документирования. И, конечно, с обучением!

Источники:
1) 2017 Norton Cyber Security Insights Report (https://us.norton.com/cybersecurity-insights-2017)
2) Kaspersky Security Bulletin: обзор 2017 года (https://securelist.ru/ksb-review-of-the-year-2017/88142/)
3) WannaCry в промышленных сетях (https://ics-cert.kaspersky.ru/reports/2017/06/08/wannacry-in-industrial-networks/)
4) IBM Future of Identity Study: Millennials Poised to Disrupt Authentication Landscape (https://www-03.ibm.com/press/us/en/pressrelease/53646.wss)
5) Mimikatz предлагает сдаться (https://www.atraining.ru/mimikatz-lsa-protection/)