УДК 004

ТЕНДЕНЦИИ ИНФОРМАЦИОННОЙ СЕТЕВОЙ БЕЗОПАСНОСТИ

Минакова Ю.В., студентка 3 курса экономического факультета
Научный руководитель - Голубев С.В., к.э.н, доцент
ФГБОУ ВО Ульяновский ГАУ

***Ключевые слова**: интернет, кибер-преступники, безопасность, компьютер.*

Сегодня интернет превращается из источника информации в виртуальное сообщество, и как в любом обществе, здесь появляются люди, которые незаконным путем пытаются получить чужую информацию для собственной выгоды. В этой работе я расскажу как обезопасить конфиденциальную информацию от тех, кто не имеет прав доступа к ней, и какие основные сетевые угрозы бывают.

На сегодняшний день нельзя представить нашу жизнь без интернета и информационных технологий. Эти вещи прочно закрепились в нашей жизни, значительно упростив ее. Любая компания и организация использует различные технические устройства, многие процессы автоматизированы, множество систем осуществляет работу по написанным программам, а человеку представляется возможностьтолько контролировать процесс исполнения деятельности, и «писать» новые программы для ещё большего ускорения процессов. С помощью современных программ, а также компьютерных технологий, человечество достигло больших высот и преобразований практически во всех сферах жизни социума. Однако, это имеет свои уязвимые аспекты: во-первых, человек стал «зависим» от технологий, во- вторых, теперь уязвимость одной технологии может привести к несостоятельности организации, и есть те, кто может этим воспользоваться в корыстных целях.

Кибер-преступники стали все более уверенными в своих силах. Хакеры практикуются и совершенствуются на более прибыльных атаках, что позволяет им получать быстрые и легкие деньги.

Хакеры переключили свое внимание на организации, которые обрабатывают огромные объемы данных, особенно персональной информации (больницы, фармацевтика, отели и т.д.). Как только они получают доступ к таким организациям, они «заражают» множество компьютеров с помощью

шифровальщиков, в результате чего могут требовать от своих жертв любые деньги в виде выкупа или продавать эти данные на «черном рынке».

1.«Шифровальщик». Класс самых популярных вредоносных программ — речь идет про трояны, которые вкупе с шифровальщиками продолжают оставаться на вершине «рейтинга» уже многие годы.

Вирусы-шифровальщики, или иначе их называют - криптографические вирусы - особый вид программного обеспечения, который осуществляет шифрование всех файлов на жестком диске. Что подразумевается под словом «шифрование»? При шифровании все файлы превращаются в набор нулей и единиц, то есть представляют собой бессмысленный набор информации, который невозможно открыть ни одной программой.Как и любой вирус, функции, который он выполняет - зависят напрямую от разработчика этого вируса.

Троян - вредоносная программа, проникающая на компьютер пользователя под безобидным внешним видом или в виде программы с каким-то осмысленным функционалом и приносящая вред.

2.Вредоносная почта. Атаки приходят не только со стороны вредоносной рекламы или взломанных сайтов. Большое количество атак все еще осуществляется через электронную почту в виде ложных счетов или различных уведомлений.

Подвох заключался в непомерно высоких суммах в счете, которые заставляли получателя возмущаться и, не думая, нажимать на ссылку для просмотра детализации. При нажатии на ссылку пользователь направлялся на ложный сайт, сильно похожий на реальный сайт обслуживающей его энергокомпании, где он мог скачать счет. Если клиент скачивал и открывал файл, то он заражался шифровальщиком.

3.Внутрикорпоративный фишинг. Злоумышленники используют перехватчики клавиатуры, почтовые сообщения, составленные по всем правилам социальной инженерии, специально разработанные веб-сайты... Чем дальше, тем изощреннее становятся методы атак, тем выше уровень их подготовленности.

4.POS-терминалы и банковские карты. Популярная сеть быстрого питания Wendy’s столкнулась с заражением вредоносными программами свыше 1000 своих PoS-терминалов, из-за чего была украдена информация о банковских картах ее клиентов.

В PandaLabs обнаружили эту атаку, выполненную с помощью известной угрозы PunkeyPOS, которая использовалась для заражения свыше 200 ресторанов в США. Еще одна подобная атака была обнаружена

нашей лабораторией в этом году. И снова пострадали рестораны в США: примерно 300 учреждений, чьи POS-терминалы были заражены с помощью вредоносной программы PosCardStealer.

5.Интернет вещей. Интернет вещей (IoT) — это следующий кошмар информационной безопасности. Любой вид устройств, подключенных к сети, может быть использован для того, чтобы проникнуть в корпоративные сети. Большинство таких устройств не имеют должного уровня безопасности.

Все это вместе делает их очень уязвимыми для внешних атак. Учитывая скорость появления уникальных вредоносных продуктов и их многообразие, защитные продукты должны быть инновационными и иметь проактивный подход в отношении обнаружения вирусных программ и других подобных угроз. Поэтому крупные антивирусные компании держат курс на развитие облачных сервисов защиты. Специалисты по вопросам информационной безопасности полагают, что за подобными технологиями будущее, т.к. большинство устройств имеют выход в Интернет. Крупные профильные представители уже представили свои «облачные» решения по информационной безопасности. Ну а мы в свою очередь можем применить: использование двухступенчатой авторизации, создание сложных паролей и запрет на использование одинаковых паролей на разных веб-сайтах — вот основные советы по сетевой безопасности, которые должны быть приняты во внимание.

Библиографический список

1. Варлатая, С.К. Защита информационных процессов в компьютерных сетях: учебно-методический комплекс / С.К. Варлатая, М.В. Шаханова.- М.: Проспект, 2015. — 216с.
2. ДиалогНаука [Электронный ресурс] // Почтовый вирус. – Режим доступа: http://www.dialognauka.ru/support/golossary/4582/
3. Софт-Архив [Электронный ресурс] // Способы распространения компьютерных вирусов. – Режим доступа: http://soft-arhiv.com/publ/4-1-0-57

TRENDS OF INFORMATION NETWORK SECURITY

Minakova Y.V.

Key words: *Internet, cyber-criminals, security, computer.*

Today, the Internet turns from a source of information in the virtual community, as in any society, there are people who are illegally trying to obtain someone else's information for their own benefit. In this work, I will tell you how to protect confidential information from those who do not have access rights to it, and what are the main network security threats are.