С.Сейфуллиннің 125 жылдығына арналған **«Сейфуллин оқулары – 15: Жастар, ғылым, технологиялар: жаңа идеялар мен перспективалар»** атты халықаралық ғылыми-теориялық конференциясының материалдары = Материалы Международной научно-теоретической конференции **«Сейфуллинские чтения – 15: Молодежь, наука, технологии – новые идеи и перспективы»**, приуроченной к 125 - летию С.Сейфуллина. - 2019. - Т.I, Ч.2 - С.139-142

АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Асылбеков У.Б.

В данной работе проведен анализ современных угроз безопасности информации с разделением их как на внутренние и внешние, с приведением примеров результатов влияния и нанесенного ущерба компаниям и предприятиям. Приведен вывод по результатам анализа и меры предостережения от описанных угроз.

Перед началом описания анализа угроз информационной безопасности в информационном пространстве, хотелось бы отметить один не маловажный момент.

Сегодня в веке технологий и инноваций человечество находится в самопоглощающем информационном потоке данных. А именно в потоке, создаваемом нами же. Человек, либо в силу стечения определенных обстоятельств, либо по роду своей профессиональной деятельности, вовлечен в среду меняющегося потока информации. Борьба за овладение ею первым идет вплоть до вылета с информационного рынка. Причина, скрывающаяся за всем этим, кроется в сегодняшнем упрощении и ускорении процесса получения информации из каких-либо необходимых источников.

Так было и в 1989 году, когда один из основателей существующей на сегодняшний день сети интернет, Тим Бернерс-Ли, работая в CERN над проектом публикации гипертекстовых документов связанных между собой гиперссылками, облегчил поиск и консолидацию информации для ученых компании.

Но, как и в любом технологическом процессе развития современного общества всегда найдется изъян способный в какой-то либо мере замедлить процесс развития, либо его ускорить. Как и в созданной сети Интернет, где информационная безопасность стала основополагающим фактором ее развития.

В данной статье приводится аналитический материал современных тенденций угроз информационной безопасности на основе обобщенных статистических данных мировых лидеров в области информационно-коммуникационных технологий и прогнозы возможной дальнейшей стратегии киберпреступников.

Современные угрозы в сфере ИБ. Если, к примеру, во временном промежутке переместиться назад на лет 5, то раньше сетевые мошенники, проникая или получая различными путями, доступ к корпоративным сетям, старались оставаться после этого незаметными, не выдавая каких-либо конкретных результатов своих действий. Сегодня же, они возможно под гидом безнаказанности потребляют мощности серверов, крадут данные и вымогают деньги у своих жертв в Интернете. При всем этом атаки с каждым разом становятся все более изощрённые и результативнее.

Перечень информационных угроз в наше время очень широк, их список ежедневно расширяется. Сегодня эти угрозы можно поделить на две основные группы: внутренние и внешние. Внешние угрозы, соответственно, исходят из «внешнего мира» (обычно из сети интернет), тогда как внутренние – угрозы, исходят из самой организации. Сегодня также выделяют еще и некоторую «промежуточную» группу угроз, которые связаны с работой провайдеров услуг. Этими услугами пользуются организации, и они дополняют её информационные ресурсы.

Внутренние угрозы. Согласно данных Глобального исследования тенденций информационной безопасности за 2017 и 2018 года заметна тенденция роста внутренних угроз от бывших сотрудников компаний. При этом среди всех источников угроз наибольший прирост (58%) в сравнении с предыдущим годом был отмечен у инцидентов, связанных с бывшими поставщиками услуг и сервисов.

Несмотря на это необходимо отметить, что заметна тенденция спада количества инцидентов ИБ в отношении действующих сотрудников. Такой не маловажный факт, как утечка информации или ее распространение по вине действующего сотрудника до сих пор актуален и предполагается, останется таким, пока существует конкуренция и соперничество.

Причиной послужившей стремительному росту уровня внутренних угроз является быстрый рост числа интеллектуальных мобильных устройств и популярности облачных вычислений, что существенно расширяет горизонт атак. С появлением принципиально новых устройств и инфраструктур перед злоумышленниками открываются новые возможности атак, использующих непредвиденные слабые места и плохо защищенные ресурсы. Так же, повсеместный доступ с мобильных устройств к служебной информации компании или к информации, которая может заинтересовать конкурирующую сторону, увеличивает риск ее хищения.

Таким образом, компании увеличивая рост бесконтрольного применения мобильных устройств для сокращения времени выполнения задач и функций, увеличивают вероятностный процент преднамеренного хищения конфиденциальных данных или атаки на внутренние информационные ресурсы. А в 100% случаях первые руководители организаций задумываются об информационной безопасности в данном моменте после возникновения инцидента ИБ.

Внешние угрозы. На практике встречаются различные типы вредоносного программного обеспечения, используемого

злоумышленниками для получения доступа к корпоративным сетям. Анализ показал, что чаще всего встречаются следующее вредоносное ПО: рекламное, шпионское, программы нежелательного перенаправления, эксплойты, использующие iFrame, и программы фишинга [1].

Список ПО можно рассматривать как коллекцию вредоностного ПО [2], используемого для получения начального доступа. Это испытанные и наиболее экономичные способы, позволяющие с легкостью скомпрометировать большие популяции пользователей. Эксплойты JavaScript и мошенничество на Facebook (социальный инжиниринг) оказались чаще всего используемыми методами атаки.

Нельзя исключать и того факта, что большему риску подвержены компании, занимающиеся какой-либо финансовой деятельностью, оперирующие конфиденциальными данными или же предоставляющие различные информационно-коммуникационные услуги широкому кругу пользователей сети Интернет.

Все вышеуказанные методики направлены на извлечение максимально возможного дохода от скомпрометированных пользователей. Злоумышленники крадут ценные данные или удерживают под контролем цифровые активы пользователей ради выкупа.

Исходя из всего, при отслеживании вредоносного ПО из Интернета, недостаточно просто сосредотачиваться на наиболее распространенных типах угроз, необходимо рассматривать полный спектр атак при организации защиты информационных ресурсов и проведения оценки эффективности ее работы по истечению заданного периода времени работы [3].

Время – деньги. Проводя анализ исследований в области информационной безопасности от крупных аналитических центров мира, следует подчеркнуть о необходимости уделять повышенное внимание ретроспективному анализу для своевременного обнаружения угроз.

Своевременные обнаружения угроз для успешного противодействия кибератакам, осуществляемые профессиональными, высоко мотивированными злоумышленниками является жизненно необходимым.

Так например, эксплойт-набор Angler, один из самых обширнейших и эффективных комплектов эксплойтов использования уязвимостей с начала 2012 года, связан с несколькими нашумевшими кампаниями незаконной рекламы и применения программ-вымогателей. Кроме того, он стал значимой составляющей общего взрывного роста активности программ-вымогателей.

Злоумышленники используют программы вымогатели для шифрования файлов пользователей, которым передаются ключи для расшифровки лишь после уплаты «выкупа» — обычно порядка 300–500 долларов [6].

Согласно результатам исследования компании Cisco, главная группа хакеров, ответственная приблизительно за половину активности эксплойтов Angler в данной кампании, атаковала до 90 000 жертв в день. По их оценке, эта кампания приносила злоумышленникам более 30 млн долл. дохода ежегодно.

Прогнозы и результаты работы по своевременному обнаружению атак на информационные ресурсы на сегодняшний день не утешительны, в виду того что время обнаружения угрозы в среднем составляет от 100 до 200 дней [6].

Вывод. Технологическая гонка между злоумышленниками и производителями решений для информационной безопасности набирает обороты, и такое положение дел лишь увеличивает риски, как для малых организаций, так и для частных лиц.

Специалисты по информационной безопасности всех уровней предприятий должны реализовывать упреждающие меры защиты. Именно использование следующих методов считаю, могут объединить в единую систему людей предприятия, ее внутренние процессы и технологии [7,8].

Комплексная защита от угроз. Использование отдельных, зачастую разнородных решений для информационной безопасности влечет за собой определенные проблемы для организаций. В связи с этим большую актуальность приобретает архитектура комплексной защиты от угроз, включающая в себя реализацию концепции повсеместной безопасности и обеспечивающая эффективность в любой контрольной точке периметра защиты.

Дополнительные меры защиты. Поддержание сетевой инфраструктуры в состоянии, отвечающей всем требованиям инфраструктуры ИБ. В том числе снижение известных уязвимостей на компьютерах, работающих в сети Интернет, а так же использование специальных средств для обеспечения интернет-безопасности.

Список литературы

1 www.hpe.com/go/hpsr. HPE Security Research. Cyber Risk Report 2015.

2 http://ponemon.org. Исследование затрат, связанных с киберпреступлениями, в 2016 году: по всему миру.

3 www.hpe.com/go/hpsr. State of Security Operations 2016 report of capabilities and maturity of cyber defense organizations.

4 www.hpe.com Companies cautiously optimistic about cybersecurity.

5 www.hpe.com. HP Security Research Cyber Risk Report 2015.

6 www.cisco.com.Годовой отчет Cisco по информационной безопасности за 2016 год.

7 www.pwc.com. Кибербезопасность в России: только факты. Ответ бизнеса на актуальные вызовы и угрозы.

8 www.pwc.ru/gsiss2016.Turnaround and transformation in cybersecurity.

Научный руководитель: ст. преподаватель, PhD Исмаилова А.А