УДК 004.031

КИБЕРБЕЗОПАСНОСТЬ ЦИФРОВОГО БИЗНЕСА МАЛОГО ПРЕДПРИЯТИЯ

Волков Е.И.

Академия экономики и управления

студент 2 курс магистратуры ЧОУ ВО ЮУ (ИУБиП)

e-mail: njvcty8olhwe@mail.ru

Научный руководитель Храмов В.В.

к.т.н., доцент кафедры «Информационные технологии и прикладная математика» ЧОУ ВО ЮУ (ИУБиП)

Аннотация: В статье рассмотрены основные положения кибербезопасности в бизнесе. Рассмотрены реальные примеры, когда бизнес пострадал от хакеров. Представлено описание основных способов реализации хакерских атак и рекомендации по предотвращению атак на малый бизнес.
Ключевые слова: кибербезопасность, хакер, угроза, атака, риск

SMALL BUSINESS DIGITAL CYBERSECURITY

Volkov E.I.

Abstract: The article discusses the main provisions of cyber security in business. Considered real examples when the business has suffered from hackers. A description of the main ways to implement hacker attacks and recommendations to prevent attacks on small business.
Keywords: cybersecurity, hacker, threat, attack, risk

Американский журнал «CSO» посвященный кибербезопасности провел опрос среди крупных и малых владельцев бизнеса [1]: Кто или что является наибольшей угрозой для информационной безопасности их фирмы? Практически все опрощенные указали на внешние угрозы, на хакеров, конкурентов и прочих недоброжелателей. И всего лишь 13% указали на своих сотрудников. Это разумный ответ, потому что даже в самой совершенной системе безопасности самым слабым звеном будет человеческий фактор [2, 3]. Но хоть человеческий фактор и будет всегда основным, не стоит полагаться лишь на знания сотрудников,

киберпреступность не стоит на месте и с каждым днем придумываются все более и более изощрённые методы взлома. Исходя из этого, высоко квалифицированные сотрудники, увлеченные своим делом, а также новейшие технологии помогут защитить свой бизнес от хакерских атак.

Из-за ошибок, допущенных собственным неквалифицированным техническим специалистом, может быть не обнаружен вирус – вымогатель. Но если администратор почистит сервер, от всех данных и самого вируса, а затем воспользуется сервисом резервного копирования, проблема будет закрыта.

Пример [4]. Небольшая компания, которая поставляла различную бижутерию, была взломана и стала заражать компьютеры своих клиентов и случайно зашедших людей вредоносным кодом. Для решения этой проблемы были наняты сотрудники со стороны, за неимением своих. Вредоносный код был удален в течение нескольких часов, однако он быстро вернулся обратно. Стало понятно: хакеры имеют доступ к сайту.

В ходе расследования выяснилось, что первым под удар попал компьютер владельца бизнеса. Он использовал бесплатный антивирус и не обновлял его своевременно, что и стало причиной реши в защите. Вредоносная программа на компьютере владельца позволила хакерам получить учетные записи сайта и базы данных [5]. Как только вредоносный код удалили, а пароли сменили, проблема, как оказалось, была устранена. Но это было только начало. Google уже внес сайт компании в черный список и удалил его из своих поисковых запросов, за наличие и распространение вредоносного кода. Так же поступили и остальные поисковые системы, яндекс, рамблер и др.

Бизнес компании оказался крайне зависим от работы сайта. За время «простоя» компания практически перестала приносить прибыль и оказалась на грани разорения. Практически год потребовался, чтобы вернуть сайт к жизни, не только в поисковые запросы, но и на те же самые позиции что он занимал раньше.

Основные типы атак киберпреступников

Киберпреступники заинтересованы в максимально эффективном и быстром похищении информации. На сегодняшний день, хакером доступен широкий перечень кибератак, который продолжает увеличивается за счёт новых технологий [6, 7]. Вот только некоторые из них:

A. Фишинг. Фишинговые атаки основываются на рассылке писем с вредоносными ссылками в них. Так же эти письма маскируют под почту различных популярных интернет – ресурсов, mail, google и прочее. Пользователь, ничего не подозревая, переходит по этим ссылкам и оставляет, тем самым, свои пароли и логины злоумышленникам.

B. DDoS атака. В ходе данной атаки, на машину или сервер предприятия отправляется сотни различных запросов одновременно, что приводит к перегрузке сервера и его полной неработоспособности. В связи с чем, ваш бизнес «простаивает» и несет убытки.

C. Malware. Вредоносный код или программа, один из самых распространённых методов организации кибератак на сайты или сервера малого бизнеса. С их помощью легко взломать ресурсы фирмы и получить доступ к конфиденциальным данным.

D. Взлом пароля. Данная кибератака основывается на подборе пароля к ресурсам фирмы. На данный момент распространены три основных метода: «кейлоггинг» – вредоносная программа, которая тайно записывает все действия пользователя за компьютером; «брутфорс» – перебор различных паролей, основанных на изучении личных данных жертвы.; «перебор по словарю» – кибератака похожая на «брутфорс», однако используется уже база данных с ранее полученными паролями.

E. Внутренняя атака. Данный тип взлома выполняется изнутри фирмы, например бывшими или действующими сотрудниками.

И это лишь основные и не многочисленные способы кибератак. Существует множество специфических атак, а также персональных, разработанных исключительно на определенную фирму или человека. Но это

не значит, что не нужно защищать свой бизнес, а наоборот, нанимать сотрудников, обучать имеющихся и самому познавать основы кибербезопасности.

Основы кибербезопасности

Простым сотрудникам и пользователям IT- ресурсов важно запомнить и выполнять шесть простых правил защиты [7, 8]. А главное, сразу сообщать о каких – либо подозрениях специалисту по кибербезопасности компании, который может провести анализ сложившейся ситуации в информационном пространстве [9, 10] локальной вычислительной сети и принять обоснованное решение. Вредоносному ПО достаточно клика, чтобы оказаться внутри сети компании.

1. Используйте сложные пароли и регулярно меняйте их.
2. Не записывайте пароли на бумаге, или на не защищенных электронных записных книжках.
3. Не используйте случайно найденные USB – накопители.
4. Не заходите на подозрительные сайты с рабочих компьютеров.
5. Не открывайте, и не нажимайте на ссылки в письмах от незнакомых людей.

Таким образом, у небольших фирм и компаний, как правило, нет средств для покупки дорогостоящего защитного ПО, а тем более на сотрудников, которые будут его поддерживать. Но если следовать этим простым инструкциям, то даже малые предприятия могут защитить себя от большинства атак извне, и смогут чувствовать себя, хоть и не в полной, но в безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИТОЧНИКОВ

1. Кузнецова И.С. Методы исследования операций для экспресс оценки бизнеса малого предприятия // Экономика и предпринимательство. – № 10-3 (75). – 2016. – С. 805-808.
2. Что такое кибербезопасность? // https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (Дата обращения 13.01.2019)

3. Храмов В.В., Трубников А.Н. Модель элементарной защиты программного средства // Информационные технологии и проблемы микроэлектроники: Сборник научных статей /под ред. докт. тех. наук, проф. В.А. Бархоткина. – Москва, 1999. – С. 192-197. https://elibrary.ru/item.asp?id=327112590 (Дата обращения 7.01.2019)
4. Носова В.. 4 правила кибербезопасности для тех, кто хочет уберечь свой бизнес // https://rb.ru/opinion/4-pravila/ (Дата обращения 7.01.2019)
5. Храмов В.В., Садовов В.В., Трубников А.Н., Губарев О.К. Защита информации в вычислительных системах: Учебное пособие для вузов. – Москва, 2002. – 192 с. https://elibrary.ru/item.asp?id=32762286 (Дата обращения 7.01.2019)
6. Храмов В.В., Трубников А.Н. Модель специальной программной закладки // Вопросы защиты информации. – 1998. – № 1-2 (40-41). –С. 36-37. https://elibrary.ru/item.asp?id=36309954 (Дата обращения 7.01.2019)
7. Киберзащита военных технологий США не поспевает за прогрессом противников // https://www.securitylab.ru/news/497665.php (Дата обращения 5.01.2019)
8. Храмов В.В. Особенности использования принципа информационного следа при поиске программных закладок // Вопросы защиты информации. 2001. – № 3(54). – С.39-40 https://elibrary.ru/item.asp?id=36312064 (Дата обращения 7.01.2019)
9. Храмов В.В. Особенности интегральной модели комплексного следа информационного объекта в условиях интеллатентности // Спектральные методы обработки информации в научных исследованиях: Доклады I Всероссийской конференции (Спектр-2000). Российский фонд фундаментальных исследований, Институт математических проблем биологии РАН. – 2000. – С. 138-140. https://elibrary.ru/item.asp?id=32657025 (Дата обращения 7.01.2019) \
10. Храмов В.В. Информационная безопасность школы: от защиты информации к политике безопасности // Информационные технологии в

образовании-2010: Сборник научных трудов участников X Южно-российской межрегиональной научно-практической конференции-выставки. 2010. – С. 218-219. https://elibrary.ru/item.asp?id=32608399 (Дата обращения 9.01.2019)