УДК 658.5 012.7

ПРОБЛЕМЫ КИБЕЗОПАСНОСТИ РОССИЙСКИХ ПРЕДПРИЯТИЙ

Анабардиева Д.О.[1]

[1]Южно-Российский институт управления- филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации «ЮРИУ РАНХ И ГС», Ростов-на-Дону, e-mail: diana.anabardieva.01@bk.ru

Аннотация: Проникновение информационных технологий во все сферы жизни общества очень сильно упростило нашу работу и дало возможность развить сферы производства и услуг до невиданных масштабов. Однако в 2020 году на фоне цифровизации мы наблюдаем глобальную пандемию COVID-19, которая заставила изменить подход не только к работе, но и к самой жизни. Вирус, передающийся прежде всего воздушно-капельным путём и обладающий высокой летальностью, заставил компании перейти на удалённую (дистанционнную) работу, а вследствие этого поспособствовал увеличению количества киберпреступлений. Необходимость выживать в условиях процветающей киберпреступности потребовала от предприятий начать поиск новых, намного более эффективных мер по защите своих данных и профилактики их утечек и сопряженных с ними финансовых потерь. В данной статье автор рассматривает пути, с помощью которых реализуется охрана компаний от инцидентов киберпреступности. Она осуществляется при помощи специальных платформ российского рынка кибербезопасности. Кроме того, что немаловажно, статья освещает наиболее распространённые сценарии атак и серьёзные риски, которые связанны с недостаточной защитой внутренних информационных систем компаний.

Ключевые слова: киберпреступность, киберугрозы, кибербезопасность, компании малого и среднего бизнеса, платформы Threat Intelligence, пандемия.

PROBLEMS OF CYBERSECURITY OF RUSSIAN ENTERPRISES

Anabardieva D.O.[1]

1South Russian Institute of management-branch of the Russian presidential Academy of national economy and public administration "YURIU RANH and GS", Rostov-on-don, e-mail: diana.anabardieva.01@bk.ru

Annotation: The penetration of information technology into all spheres of society has made our work much effortless and has made it possible to expand production and services to an unprecedented scale. However, in 2020, against the backdrop of digitization, we are witnessing the global COVID-19 pandemic, which has changed the way we look not only at work but also at life itself. The virus, which is primarily airborne and highly lethal, has forced companies to work remotely and has contributed to an increase in cybercrime. The need to survive a thriving cybercrime environment has required firms to start looking for new and much more effective measures to protect their data and prevent leaks and associated financial losses. In this article, the author examines how companies are protected from cybercrime incidents. It is implemented through specific platforms of the Russian cybersecurity market. Besides, and importantly, the article highlights the most common attack scenarios and the risks associated with the lack of protection of companies' internal information systems.

Keywords: cybercrime, cyber threats, cybersecurity, small and medium-sized businesses, Threat Intelligence platforms, pandemic.

Информационные технологии сегодня проникают во все сферы жизни, упрощают нашу работу, дают предпринимателям, компаниям и государствам огромные возможности для развития сфер производства и услуг. С. Плуготаренко, директор Ассоциации электронных коммуникаций как-то произнес: «За Интернетом шаговой доступности пришли угрозы шаговой доступности». Помимо плюсов, в цифровизации есть и существенные минусы. И в первую очередь это касается проблемы киберугроз и киберпреступности, так как они несут особый урон не только экономике страны, но и государству в целом. Особенно серьёзна и актуальна их проблема на фоне пандемии, которая вынудила работать большинство фирм удаленно, потому она требует немедленного решения. В России Правительство уже предприняло ряд мер по борьбе с киберпреступностью и

обеспечению ИБ, к таким относятся раздел «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации». В новых приказах 2019-2020 года № 277,891,755,705 содержится информация о субсидиях, предоставляемых на развитие ИБ, создания киберполигонов для подготовки специалистов по кибербезопасности и т.д. Но одним из основополагающих законов, принятых государством, на мой взгляд, является Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ вступил в силу 1 января 2018 года.

Для того, чтобы понять, как бороться с кибератаками, необходимо знать, что же такое: киберпреступность и кибербезопасность. Если киберпреступность означает совершение кибератак за счет применения вредоносных программ на слабые места в аппаратном и программном обеспечении, то кибербезопасность, напротив, борется с этими преступлениями, посредством защиты данных. Сегодня технические системы предприятий подвержены риску киберугроз со все более новыми способами взлома.

Совместно проведенное TAdviser и Microsoft аналитическое исследование в 2019 году, посвященное кибербезопасности в российских компаниях малого и среднего бизнеса, показало неутешительные результаты. По полученным данным, за год с целенаправленными атаками столкнулись 39% компаний сегмента СМБ, при чем компания Positive Technologies, выявила что более 50% СМБ-компаний присваивают риску APT-атаки высокий уровень опасности.

В результате проведенного нами анализа данных, было выяснено, что число атак во 2 квартале 2020 выросло на 9% по сравнению с I кварталом и на 59% по сравнению с аналогичным периодом 2019 года. Специалисты и аналитики связывают рост числа кибератак с пандемией, поскольку она создала благоприятную почву для применения злоумышленниками методов социальной инженерии. На апрель и май 2020 года выдалось рекордное число успешных киберпреступлений. Специалисты отметили, что около половины (46%) атак с использованием ВПО пришлись на шифровальщиков, еще 41% — это атаки шпионских троянов. Исследование TAdviser и Microsoft также выявило, что основными каналами угроз стали: электронная почта (66%) и внешние интернет-ресурсы (63%), далее следуют внешние накопители (18%) и мессенджеры (10%).

Важно отметить, что проведенный анализ Positive Technologies «APT-атаки глазами сотрудников российских компаний» показал, что компании малого и среднего бизнеса осознают, насколько серьезна проблема киберпреступности, поскольку ее последствия оказываются очень тяжелыми, а иногда и фатальными для сегмента малого и среднего бизнеса. Кроме утечки информации и финансовых потерь наблюдаются и другие не менее тяжелые последствия, которые приведены мной в диаграмме (Рис.1.):

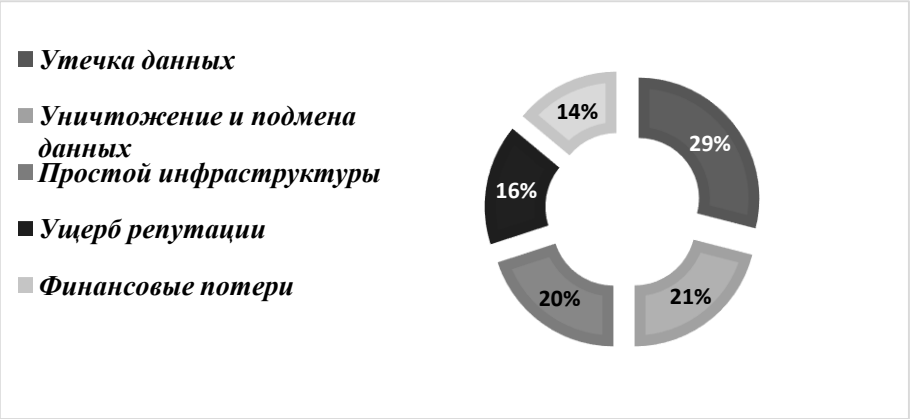

Рис 1. Последствия киберугроз.

Интересным наблюдением стало замечание специалистов программ ИБ Microsoft, которые прокомментировав результаты исследования, отметили то, что рост интереса киберпреступников к СМБ-компаниям, во многом благодаря ИТ-неграмотным сотрудникам компаний, которые не обучены новых технологическим введениям или плохо владеют компьютерами и цифровыми носителями информации. Именно они становятся легкой мишенью киберпреступников, использующих методы социальной инженерии. За 2018 год среднемесячный показатель подобных атак вырос в 4,5 раза. Следовательно, можно сделать вывод, что оснащение предприятий грамотными специалистами скорее сейчас становится необходимостью для работы компаний.

В исследовании хотелось бы рассмотреть наиболее распространенные сценарии атак 2020 года, от которых российские предприятия СМБ во время пандемии пострадали больше всего:

1. **Взлом веб-ресурсов и кража базы учетных данных.** Отмечается, что жертвами преступлений становились преимущественно интернет-магазины и организации сферы услуг, онлайн-сервисы (например, кэшбек-сервисы). В основном было выявлено, что атаки осуществлялись через нахождение слабых мест в системе данных или же с помощью подбора пароля для доступа к сайтам.
2. **Фишинговые письма со ссылкой на поддельную форму аутентификации.** Важно отметить, что, в большинстве случаев, злоумышленники подделывают формы аутентификации продуктов Microsoft — Office 365, Outlook, SharePoint. Однако на фоне пандемии для кражи данных популярностью у киберпреступников стали пользоваться системы аудио- и видеосвязи, такие как Zoom, Microsoft Teams.
3. **Заражение вредоносным ПО, похищающим учетные данные.** Довольно частым стало явление, когда работники, открыв вложения фишинговых писем заражают систему вредоносными программами, через которые злоумышленники похищают множество документов компании и учетные записи сотрудников.

Теперь разберемся, как уменьшить риск кибератак СМБ-компаний. Для этого обратимся к данным исследования Positive Technologies, которое показывает, какие типовые средства защиты ими в большинстве случаев уже используются (Рис.2.).

Рис 2. Типовые средства защиты от киберпреступности.

Можно заметить, что на долю специализированных решений для защиты от APT приходятся только 9%. Конечно, очень важно, что сегодня умные и профессионально-грамотных предпринимателей, которые осознают риск APT становится все больше, однако на практике подход к обеспечению безопасности пока не соответствует новым угрозам со стороны киберпреступников, так как эффективное новое ПО по карману не всем компаниям малого и среднего бизнеса. Из-за этого страдает и инфраструктура рынка.

На основании проведенного нами исследования киберпреступлений 2020 года были выявлены базовые способы киберзащиты, которые, на наш взгляд, должны осуществляться компаниями, чтобы хотя бы минимально обезопасить свои данные: обучение сотрудников кибербезопасности, ввод авторизации с разными уровнями доступа; необходимо использовать только лицензионное ПО, вовремя его обновлять, и только из надежных источников, антивирусные программы, выстраивать защиту в несколько «слоев»; после каждой кибератаки проводить анализ информационной безопасности компании и принимать меры по ее улучшению.

Но, на наш взгляд, данных мер недостаточно в условиях быстрого развития киберпреступности. Поэтому необходимо производить правильную настройку технических средств защиты, постоянный сбор и обработку информации о событиях безопасности, анализ трафика и поиск подозрительной активности в инфраструктуре и много чего еще. Все это может обеспечить специальная платформа. В России рынок платформ Threat Intelligence находится на стадии развития, однако несколько крупных вендоров уже успели представить свои разработки. В результате исследования было выявлено, что лидерами являются: Kaspersky Threat Intelligence; R-Vision Threat Intelligence; Solar MSS. Стоит сказать, что стоимость многих из этих платформ достаточно высока для компаний СМБ.

1. Kaspersky Threat Intelligence является особенным сервисом по борьбе с кибергрозами, так как основное его преимущество - оперативное реагирование на попутку взлома, с последующим эффективным расследованием его появления. Предоставляет пользователям постоянно обновляемую информацию по киберпреступникам, статистике и активности преступлений, благодаря чему специалисты по реагированию на киберугрозы могут быстро отследить угрозу, проанализировать ее характер, нацеленность и степень риска для безопасности, изучить тактику атакующего, и что самое главное, отыскивать методы борьбы с ним. Все это повышает качество расследования инцидентов.

2. R-Vision Threat Intelligence Platform платформа, которая очень схожа с предыдущей, но достаточно сказать, что менее оперативна в сравнении с Kaspersky. Но ее особенностью является то, что сервис в автоматическом режиме собирает данные из источников и анализирует взаимосвязи кибератак, позволяя аналитику получить целостное представление об угрозе.

3. Заключительной платформой является Solar MSS. Это новый для рынка формат предоставления услуг класса «кибербезопасность как сервис», ориентирован на более массовый корпоративный сегмент, предприятий СМБ, имеет относительно невысокую цену. Solar MSS предоставляет услуги по кибербезопасности «из облака», обеспечивая надежность и защищенность каналов связи, а также возможность централизованно управлять всеми сервисами.

Таким образом, подводя итог всему вышесказанному, мы видим, что количество случаев целенаправленных кибератак на компании СМБ учащается, в связи с переходом компаний на дистанционную работу. Самым эффективным методом борьбы является хорошее техническое обеспечение, которое можно купить на российском рынке платформ кибербезопасности. Самым бюджетным и базовым по выполняемым функциям является выбор платформы Solar MSS. И важно помнить, что издержки по принятию мер защиты цифровой стороны бизнеса не встанут в сравнение с затратами на устранение последствий удачных для злоумышленников кибератак. Поэтому одной из первостепенных задач для компаний становится проблема установления качественной защиты для успешного дальнейшего ведения бизнеса.

Список используемой литературы:

1. Сапрыкина А. Российские компании готовы к киберугрозам//ComNews.11.09.2020. URL: https://www.comnews.ru/content/209027/2020-09-11/2020-w37/rossiyskie-kompanii-gotovy-k-kiberugrozam (18.12.2020)

2. Дубенсков П. Программно-определяемый подход обеспечивает свободу цифрового развития// TAdviser.2020.URL: https://www.tadviser.ru/index.php/Статья:39_российских_СМБ-компаний_столкнулись_с_целенаправленными_кибератаками (19.12.20)

3. Дубенсков П. Кибербезопасность как сервис – теперь не только для крупного бизнеса// TAdviser. 2020.URL: https://www.tadviser.ru/dex.php/Статья:Кибербезопасность как сервис теперь не только для крупного бизнеса (18.12.2020)

4. Positive Technologies. Актуальные киберугрозы II квартал 2020 года// Cybersecurity_threatscape-2020. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-threatscape-2020-q2-rus.pdf (20.12.2020)

5. Шеремет И.А. Обеспечение кибербезопасности в условиях развития цифровой экономики // Вестн. Моск. ун-та.. 2019. № 1.https://cyberleninka.ru/article/n/obespechenie-kiberbezopasnosti-v-usloviyah-razvitiya-tsifrovoy-ekonomiki (19.12.2020)