УДК 004 **Информационные технологии**

Капитанчук Василий Вячеславович, *доцент кафедры организации аэропортовой деятельности и информационных технологий, кандидат технических наук, доцент, Ульяновский институт гражданской авиации имени главного маршала авиации Б.П. Бугаева, Россия, г. Ульяновск*

Кононов Никита Алексеевич, *курсант 3 курса, группы АБ-19-1 по профилю подготовки обеспечение авиационной безопасности, Ульяновский институт гражданской авиации имени главного маршала авиации Б.П. Бугаева, Россия, г. Ульяновск*

Колесников Павел Сергеевич, *курсант 3 курса, группы АБ-19-1 по профилю подготовки обеспечение авиационной безопасности, Ульяновский институт гражданской авиации имени главного маршала авиации Б.П. Бугаева, Россия, г. Ульяновск*

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКИХ СИСТЕМ

Аннотация: Цель статьи заключается в ознакомлении читателей с существующими видами кибератак и мерами и инструментами, которые позволяют с ними справляться. Раскрывается важность цифровой гигиены сотрудниками финансовых организаций, и возможные последствия при её несоблюдении.

Ключевые слова: кибератака, кибербезопасность, финансовые организации, банк, программы-вымогатели, спуфинг, фишинговые атаки, цифровая гигиена.

Annotation: The purpose of the article is to familiarize readers with the existing types of cyber attacks and measures and tools that allow them to cope with them. The importance of digital hygiene by employees of financial organizations is revealed, and the possible consequences of its non-compliance.

Keywords: cyberattacks, cybersecurity, financial organizations, bank, ransomware, spoofing, phishing attacks, digital hygiene.

В настоящее время люди настолько привыкли пользоваться банковскими счетами, пластиковыми картами, электронными платежными системами, что они даже не придают этому особого значения, это стало обыденностью.

Современный человек почти полностью перешел на безналичную оплату, без которой представить свою жизнь многим уже просто невозможно. Вместе с тем, как развивается цифровое общество, возрастают угрозы киберпреступности. Применение современных средств защиты персональных данных граждан является наиболее значимой задачей для банковских служб кибербезопасности. Банковские службы кибербезопасности определяют безопасность наших персональных данных и, соответственно, нас самих.

Исследование американского медиа-холдинга S&P Global о количестве зарегистрированных кибератак в самых разнообразных отраслях за последние пять лет с 2016 по 2021г показало, что финансовые организации занимают верхние строчки списка отраслей наиболее подверженных кибератакам, они подвергаются более чем 25% всех осуществляемых кибератак [4].

Стремительные темпы роста объема киберугроз говорят о важности разработки и применения современных методов кибербезопасности. Кибератаки способны наносить непоправимый ущерб, в особенности малым финансовым организациям, не имеющим достаточного количества средств и ресурсов для их преодоления. Кроме всего прочего, ущерб, нанесенный репутации подобным финансовым организациям, может быть фатальным [3].

Финансовые организации все чаще имеют дело с серьезными киберугрозами разного рода, которые можно преодолеть при помощи высокоэффективных стратегий кибербезопасности. В данной статье будут рассмотрены средства, позволяющие наиболее эффективно справляться с кибератаками, а также инструменты, направленные на укрепление кибербезопасности финансовых организаций.

1. Вброс учетных данных

Вброс учетных данных – это кибератака, при осуществлении которой происходит кража списков идентификаторов электронных почт, а также имен и паролей пользователей с целью получения доступа к учетным записям пользователей при помощи огромного количества запросов на вход. В финансовых организациях вброс учетных данных позволяет получить доступ к персональным идентифицируемым данным клиентов. Полученная таким образом информация в дальнейшем может использоваться при взломе веб-сайтов и серверов, с целью получения доступа к критической IT-инфраструктуре.

Логины и пароли, получаемые через «теневой интернет», позволяют сэкономить время злоумышленникам, так как эти данные учетных записей когда-то были в обороте, и вероятность повторного использования этих данных довольно высокая. Вброс учетных данных несет реальную угрозу, при реализации которой может произойти массовая утечка персональных данных.

2. Фишинговые атаки.

Фишинговые атаки являются самым массовым видом кибератак, это обусловлено их простотой. Они позволяют злоумышленникам получать большое количество персональных данных. Осуществление такой кибератаки происходит после открытия ссылки, содержащей фишинговое программное обеспечение, которое встраивается в систему.

Фишинговые атаки несут серьезные последствия для финансовых организаций, так как, если их своевременно не выявить, то фишинговое ПО имеет возможность остаться во внутренней сети организации и в последствии организовать атаку крайне большого масштаба, в таком случае эта угроза будет носить название постоянной серьезной угрозы. При осуществлении такого сценария злоумышленник имеет возможность завладеть доступом к системе организации и остаться незамеченным. Подобный сценарий может привести к крайне серьезным последствиям, начиная от финансовых потерь, заканчивая репутационными.

3. Банковские трояны.

Задумка троянского коня имеет историческое происхождение, в троянской войне греки преподнесли в виде подарка большую деревянную лошадь, внутри которой были бойцы, и попали в город Троя. В наше время «троянский конь» описывает стратегии, при помощи которых злоумышленник имеет возможность посредством обмана завладеть тем, что ему необходимо.

Банковский троян - вредоносное компьютерное ПО, позволяющее получить доступ к конфиденциальной информации и персональным данным клиента банка, обрабатываемым при помощи систем онлайн-банкинга. Этот вид вредоносного ПО имеет BackDoor, это значит, что доступ к компьютеру, зараженному данным ПО, имеет сторонний человек.

4. Программы-вымогатели.

Программа-вымогатель – вредоносное ПО, блокирующее доступ к данным для владельцев этих данных до момента внесения платы, необходимой для разблокировки заблокированных данных. Это достаточно распространенная угроза для финансовых организаций, в прошедшем (2021) году большинство финансовых организаций регулярно сталкивались с программами-вымогателями.

Программы-вымогатели создают угрозы не только в банковских учреждениях, а также на криптовалютных платформах, так как их децентрализованный характер позволяет злоумышленникам блокировать доступ администраторов любых торговых платформ к необходимым им данным и завладевать денежными средствами путем вымогательства.

Внутреннее устройство криптовалют позволяет программам-вымогателям не раскрывать своих владельцев, что позволяет злоумышленникам атаковать любую платформу, структуру, организацию, без страха быть замеченными правоохранительными органами.

5. Спуфинг.

Данный тип кибератаки подразумевает создание сайта, идентичного сайту финансовой организации, другими словами сайт-близнец. Данный сайт

выглядит и преподносит себя как настоящий официальный сайт финансового учреждения. Создается домен с очень незаметным изменением в написании, к примеру оригинальный домен выглядит «ollo-bank.ru», домен злоумышленников «olio-bank.ru», либо же меняется расширение домена с «ollo-bank.ru» на «ollo-bank.com». Ссылки на подобные сайты рассылаются на электронные почты или же на телефон в виде смс-сообщения с неизвестного номера. Пользователь, который не имеет информации о существовании подобных сайтов, вводит свои регистрационные данные, которые тут же попадают в руки злоумышленников. Как правило для отражения подобных атак хватает простой многофакторной аутентификации, к примеру, после ввода регистрационных данных сайт финансового учреждения отправляет одноразовый код в смс-сообщении на номер, привязанный к учетной записи пользователя, и запрашивает его для входа в учетную запись.

Все перечисленные угрозы, разумеется, необходимо взять под особый контроль специалистам банковских служб кибербезопасности. От того какие меры в области кибербезопасности принимает финансовая организация зависит ее жизнеспособность на финансовом рынке. Поэтому необходимо реализовать эффективные организационные и технологические решения, во избежание потенциальных проблем, связанных с безопасностью в системе передачи данных того или иного финансового учреждения.

Как правило объектами атак злоумышленников становятся небольшие банки и кредитные союзы, поскольку в них зачастую отсутствует надежная система кибербезопасности, позволяющая предотвратить вторжение злоумышленников, именно это и привлекает киберпреступников.

Киберугрозы в современном мире принимают крайне широкий масштаб, однако, существуют меры, позволяющие устранять угрозы кибербезопасности в банках:

1. Оценка текущего состояния облачной безопасности по сравнению с контрольными показателями безопасности, современными практиками и стандартами соответствия.

2. Поддержание всех систем в актуальном состоянии, с целью сведения к минимуму уязвимости и избежания загрузки неопубликованных приложений, чтобы свести к минимуму вероятность атак с нулевым кликом.

3. Создание структурированного плана аварийного восстановления, во избежание массовой потери данных и простоев в случае кибератаки.

4. Использование инструментов управления уязвимостями для автоматизации обнаружения угроз и защиты от потенциальных угроз.

5. Установка параметров автоматического резервного копирования с безопасным шифрованием и управлением привилегированным доступом.

6. Создание системы контроля доступа для работников, работающим неполный рабочий день, временным работникам и сторонним поставщикам.

7. Использование криптографического шифрования [1].

Большинство пользователей использует одни и те же пароли, не меняя их с течением времени. Что делает их учетные записи уязвимыми к получению несанкционированного доступа злоумышленником. Для повышения безопасности учетных записей необходимо вводить многофакторную аутентификации в роли дополнительного уровня защиты, это существенно снизит вероятность взлома учетной записи.

Помимо этих мер, имеются некоторые инструменты, применимые для укрепления кибербезопасности раздичных финансовых организаций:

1) банкам и различным финансовым организациям необходимо иметь эффективные инструменты кибербезопасности. Сотрудникам банковских служб кибербезопасности стоит проводить аналитику, чтобы понимать, какие меры эффективны, а какие нет, с целью дальнейшего повышения эффективности тех или иных мер, путем изменения старых, или введения новых;

2) имеет смысл внедрять продукты Network Insight или им подобные. Продукты Network Insight – инструменты, предоставляющие централизованное представление сетевых данных финансовой организации с целью определения потенциальных угроз кибербезопасности. Своевременное выявление

уязвимостей позволяет предупреждать реализацию кибератак, путем устранения найденных уязвимостей;

3) необходимо своевременно обнаруживать и останавливать утечку персональных данных. Технологии, позволяющие это осуществлять называются DLP;

4) высокоэффективны инструменты сбора информации о киберпреступлениях. Они предполагают круглосуточный контроль «теневого интернета». Данные инструменты позволяют повысить уровень кибербезопасности в финансовых организациях, уменьшить количество киберпреступлений, и своевременно узнавать о произошедших киберпреступлениях, после чего с помощью инструментов анализа сделать выводы и внести изменения для устранения уязвимости;

5) довольно эффективны инструменты, основывающиеся на машинном обучении. Они занимаются отслеживанием модели расходов клиентов и позволяют обнаружить момент, когда учетные записи пользователей были как-либо скомпрометированы. Своевременная информация о актах мошенничества позволяет финансовым организациям оперативно пресекать подобные случаи до того, как ущерб станет значительным.

Руководства финансовых организаций прекрасно осознают, ответственность, возлагаемую на них, а также уровни рисков, с которыми им приходится сталкиваться в связи с высоким уровнем киберпреступности. По этой причине банки и прочие финансовые организации научились адаптироваться к постоянно изменяющимся стандартам удаленной работы.

Меры, применяемые для повышения кибербезопасности в современных финансовых организациях:

1. Качественное обучение и различные поощрения за соблюдение цифровой гигиены, а также наказания в случае ее несоблюдения.
2. Использование новейшего лицензионного ПО, а также своевременное его обновление.
3. Изменение политик кибербезопасности.

4. Использование только проверенных USB-устройств.

5. Использование многофакторной аутентификации, включающей биометрию.

6. Инвестирование в разработку искусственного интеллекта для своевременного обнаружения актов мошенничества, а также их оперативного пресечения.

7. Увеличение графы расходов в области кибербезопасности [2].

Подводя итог, можно сказать, что тема кибербезопасности в современном мире крайне актуальна. Огромное количество кибератак в наше время, подталкивает банковские и прочие финансовые организации всерьез заняться кибербезопасностью, с целью предупреждения этих самых атак.

Внедрение новейших мер и инструментов по повышению кибербезопасности в той или иной финансовой организации, позволяет завоевать как можно больше клиентов с помощью репутации надежного финансового учреждения. Что в свою очередь позволяет привлечь новые инвестиции.

Библиографический список:

1. Бердюгин А.А., Ревенков В.П. Оценка риска воздействия кибератак в технологии собственного банкинга (пример программной реализации) // Финансы: теория и практика. 2020. №6.

2. Приходько А.А., Керопян Г.Б. Потери банков от киберпреступности // StudNet. 2020. №12.

3. Калашников М.М. Будущее оптимизации банковских рисков // E-Scio. 2021. №1.

4. [Электронный ресурс] – Режим доступа. - URL: https://www.spglobal.com/ratings/en/research/articles/210524-cyber-risk-in-a-new-era-the-effect-on-bank-ratings-11946210 (Кибер-риск в новую эпоху) (дата обращения 10.03.2022).