УДК 004.056

Савельев Максим Александрович
специалист
Московский физико-технический институт (государственный университет);
менеджер продукта
Donnelley Financial Solutions
Savelyev Maksim
Specialist
Moscow Institute of Physics and Technology (State University);
Product Manager
Donnelley Financial Solutions

DOI: 10.25313/2520-2057-2021-1-6824

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПОЛЬЗОВАТЕЛЕЙ В ПЕРИОД ПАНДЕМИИ COVID-19

THE PROBLEM OF PROVISION OF THE INFORMATION SECURITY OF USERS DURING THE COVID-19 PANDEMIC

Аннотация. *Статья посвящена проблеме обеспечения информационной безопасности корпоративных пользователей в период глобальной пандемии Covid-19. В статье приведен анализ актуальных угроз информационной безопасности, а также рассматриваются рекомендации по минимизации инцидентов информационной безопасности.*

Ключевые слова: *информационная безопасность, covid-19, угроза безопасности, фишинг, сетевая инфраструктура, кибербезопасность.*

Summary. *The article is devoted to the problem of provisioning the information security of corporate users during the global Covid-19 pandemic. The article provides an analysis of relevant threats to information security, and also discusses recommendations for minimizing information security incidents.*

Key words: *information security, covid-19, security threat, phishing, network infrastructure, cybersecurity.*

Пандемия коронавируса (Covid-19), случившаяся в 2020 году, стала беспрецедентным по своему масштабу кризисом, повлиявшим не только на здоровье миллионов людей по всему миру, их привычный уклад жизни, но и на экономику отдельных компаний и стран. В отличие от эпидемий и экономических кризисов прошлых лет, текущий кризис стал для многих не только финансовым потрясением, но и оказал и оказывает до сегодняшнего дня глубокое воздействие на повседневные процессы функционирования бизнеса, меняя их коренным образом. Многие компании, для обеспечения непрерывности оказания услуг и защиты своих сотрудников от риска заражения, стали в экстренном порядке переводить значительную часть сотрудников на удаленный режим, что вызывало резкий рост использования цифровых инструментов в работе, в том числе для организации каналов коммуникации [1]. Эти и прочие изменения являются благодатной почвой для появления новых типов и способов реализации угроз информационной безопасности злоумышленниками.

До начала нынешнего кризиса одной из причин реализации кибератак в корпоративной сфере являлось отсутствие комплексного подхода к организации мер по защите информации на предприятиях. Особенно ярко это можно увидеть на примере предприятий малого и среднего бизнеса, которые, как правило, не имеют совсем или имеют фрагментарный подход к организации кибербезопасности. Так, согласно отчету Verizon 2019 г. [2], более 40% кибератак в США направлены на предприятия малого бизнеса, со средним размером потерь от атаки в 188 тысяч долларов для бизнеса. Крупный бизнес также потенциально несет эти риски, несмотря на

зачастую более формализованный подход к обеспечению информационной безопасности — малые предприятия являются ключевыми участниками цепочек, так что компрометирование одного элемента вызывает риски для всех участников.

Рассмотрим потенциальные угрозы информационной безопасности бизнеса, которые стали актуальными в связи изменениями, вызванными глобальной пандемией:

- Рост нагрузки на сетевую инфраструктуру и элементы управления VPN корпоративных сетей, по причине увеличения количества сотрудников, работающих удаленно.
- Отсутствие или проведение недостаточно глубокого анализа угроз информационной безопасности и необходимых мер по ее обеспечению, при экстренном переводе сотрудников на удаленную работу и выстраиванию бизнес-процессов.
- Отсутствие плана по реагированию на совершенные кибератаки, минимизации их последствий и восстановлению работоспособности цифровой среды предприятия.
- Низкий уровень осведомленности сотрудников об угрозах информационной безопасности и мерах предосторожности при работе в дистанционном режиме.
- Ограниченные возможности по контролю безопасности личных домашних сетей сотрудников, которые они используют для подключения к корпоративным ресурсам.
- Повышение риска компрометации контрагентов, клиентов и прочих участников цепочек поставок, снижение уровня доверия к третьим сторонам с точки зрения кибербезопасности.
- Сокращение операционных расходов компаний, в том числе расходов на содержание функции информационной безопасности, из-за негативной экономической ситуации, вызванной эпидемией.

Данные угрозы носят комплексный характер и при различных условиях могут проявлять как угрозы конфиденциальности, так и целостности или доступности. Не являясь принципиально новыми сами по себе, они крайне актуальны для компаний, ранее не уделявших должного внимания кибербезопасности, но столкнувшихся с необходимостью перевода процессов в онлайн-режим.

Изменение цифрового ландшафта в связи с пандемией не вызвало появления принципиально новых типов атак, однако еще больше выделило среди них атаки, основанные на социальной инженерии. Это связано, прежде всего, с ростом количество пользователей, чья деятельность вынужденно была переведена в онлайн-режим, а также тех, кто имеет меньший опыт и знания о мерах предосторожности. Согласно исследованию Kaspersky в 2018 году, более 50% инцидентов информационной безопасности были так или иначе связаны с человеческим фактором [3]. Ярким представителем такого рода атак является фишинг и компрометация корпоративной электронной почты. Фишинговые атаки отличаются тем, что они очень быстро адаптируются к меняющейся обстановке и способны быстро распространяться во время кризисов. В случае пандемии произошел большой всплеск почтовых рассылок, в которых у пользователей запрашивалась конфиденциальная информация или их просили перейти по вредоносным ссылкам под предлогом запросов официальных органов власти или здравоохранения. В таких условиях, когда люди не имеют актуальной и достоверной информации, либо не осведомлены о происходящих событиях, они особенно уязвимы. Другой вариацией атак является рассылка вредоносного программного обеспечения также под предлогом запроса от официальных лиц. Внедрение такого рода ПО в корпоративную сеть может привести к компрометации или потере конфиденциальной информации и нанести значительный урон бизнесу компании.

С учетом указанных выше потенциальных угроз и атак на программную среду компаний рассмотрим рекомендации, которые могут быть использованы для минимизации риска реализации угроз или уменьшению возможные потери от них.

Базовой рекомендацией является установление формальных политик информационной безопасности в компании и контроль за их выполнением. Политики должны быть утверждены на уровне компании и распространяться на всех сотрудников.

Главным шагом по обеспечению безопасности является информирование сотрудников о важности этой проблемы. Важно отметить, что человеческий фактор всегда является ключевым в вопросах безопасности, и при отсутствии элементарного понимания у сотрудников о мерах предосторожности, невозможно говорить о какой-либо надежной политике безопасности в компании. Сотрудники должны четко понимать свои ежедневные обязанности по обработке, защите и использованию корпоративных данных. Это включает в себя и использование надежных паролей, игнорирование фишинговых писем и подозрительных сайтов, или установку нелицензионных программ.

Сотрудники — это всегда первая и самая главная линия обороны против кибератак. Со своей стороны, сотрудники подразделений информационной безопасности должны обучать пользователей, проводить регулярную коммуникацию, подсвечивая важность этой проблемы [4].

Другой аспект, особенно актуальный во время массовой дистанционной работы — усиление политик и процедур удаленного доступа. Сотрудники могут использовать большое количество различных устройств (личные или корпоративные компьютеры, телефоны, планшеты и прочее), различные сети (домашние, публичные, выделенные каналы) для доступа к данным и ресурсам компании. В этих условиях

важны как организационные, так и технические аспекты доступа. Общая рекомендация включает предпочтительное использование корпоративных устройств, в сравнении с личными, а и использование ресурсов вне корпоративной сети должно происходить через надежно защищенный VPN канал [5].

Среди прочих рекомендаций, которые должны быть формализованы в политику безопасности компании — это инструкции и планы по реагированию на инциденты безопасности и отлаженные механизмы по восстановлению данных [5].

Отдельно стоит отметить о необходимости защиты информации, поступающей от клиентов и контрагентов. Крайне важно, чтобы все публичные точки входа в информационный сегмент компании (порталы поставщиков, клиентские веб-сервисы) строго оценивались с точки зрения угроз, контролировались и защищались должным образом. В качестве базовых рекомендаций стоит упомянуть своевременное обновление программного обеспечения и использование многофакторной аутентификации пользователей.

Вопрос обеспечения информационной безопасности с каждым годом становится только актуальнее, несмотря на непрекращающееся развитие средств защиты. Злоумышленники каждый день придумывают новые способы получить доступ к нашим данным, используя всевозможные для этого методы, поводы и события в окружающим мире. Из-за последствий эпидемии в 2020 году весь мир особенно ярко увидел, что диджитализация всех сфер жизни — это естественный процесс, к которому мы идем, и, что проблема кибербезопасности касается каждого, а не только отдельных людей или специалистов. Умение защитить себя и свои данные на сегодняшний день — это необходимый навык для каждого, и чем раньше большинство людей это осознают, тем легче им будет освоиться в цифровом мире.

Литература

1. Conger S. The Impact of the COVID-19 Pandemic on Information Systems Management. 2020 // Information Systems Management. 2020. URL: https://doi.org/10.1080/10580530.2020.1820636 (дата обращения обращения 03.01.2021)

2. Verizon 2019 Data Breach Investigations Report. URL: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf (дата обращения 03.01.2021)

3. Applied Risk's the State of Industrial Cyber Security 2019. URL: https://applied-risk.com/resources/the-state-of-industrial-cyber-security-2019 (дата обращения обращения 03.01.2021)

4. Об угрозах безопасности информации, связанных с пандемией коронавируса (COVID-19.). НКЦКИ, 2020. 2–4 с. URL: https://safe-surf.ru/upload/ALRT/ALRT-20200320.1.pdf (дата обращения обращения 03.01.2021)

5. Рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры. ФСТЭК России, 2020. Письмо ФСТЭК России от 20 марта 2020 г. N 240/84/389. URL: https://fstec.ru/component/attachments/download/2711 (дата обращения обращения 03.01.2021)