информации. Это и обуславливает высокий спрос и актуальность использования дата-центров. [3]

Литература

1. Дата-центры: рынок растет, спрос увеличивается [Электронный ресурс]. –2021–. Режим доступа: https://skladium.ru/rynok/datacenters-rynok-rastet-spros-uvelichivaetsya. - Дата доступа: 18.03.2021.

2. Что такое дата-центр и почему он необходим сегодня бизнесу? [Электронный ресурс]. –2021–. Режим доступа: https://gigacenter.ua/ru/news/chto-takoe-data-centr-i-pochemu-on-neobhodim-segodnya-biznesu/ - Дата доступа: 18.03.2021.

3. Что такое ЦОД (Центр Обработки Данных) [Электронный ресурс]. – 2021–. Режим доступа: https://www.dataspace.ru/company/press-center/chto-takoe-cod/ - Дата доступа: 18.03.2021.

БЕЗОПАСНОЕ ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННОЙ ПОЧТЫ (E-MAIL). ВЫБОР ПОЧТОВОГО КЛИЕНТА. ЗАЩИТА ОТ СПАМА

Можейко Е.А., Жуковская Е.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Многие компании зачастую используют электронную почту (Email) для внутреннего общения с сотрудниками и внешнего – с клиентами и поставщиками. Как правило, большинство людей дважды не думают об электронных письмах, которые они отправляют в течение дня, или о вложениях, которые прикрепляются к этим сообщениям. Безопасность электронной почты, безусловно, улучшилась с момента её создания (например, реализация зашифрованных паролей). Однако, на сегодняшний день электронная почта не является полностью безопасным способом передачи важной информации. [1]

Например, электронное письмо не просто мгновенно доставляется от отправителя к получателю. На самом деле, большинство писем должны «путешествовать» по нескольким сетям и серверам, прежде чем попасть в почтовый ящик к своему получателю. Эти «точки паузы» подвергают электронную почту атаке, как правило, из-за незащищённых сетей, уязвимых серверов, а также из-за людей (хакеров), которые взламывают сеть/сервер. Более того, поскольку сообщения электронной почты обычно не шифруются, хакеры, которым удаётся проникнуть в сеть или сервер,

могут легко прочитать эти письма, а также любые сопутствующие вложения. Некоторые серверы хранят электронные письма десятилетней давности, а некоторые – письма, которые были фактически удалены в какой-то момент. Даже если хакеры напрямую не нацеливаются на сообщения электронной почты и не получают их, они могут использовать пароль, необходимый для входа в учётную запись электронной почты, поскольку многие провайдеры не требуют двухфакторной аутентификации. [4]

Кроме того, отправив электронное письмо, отправитель не может запретить получателям дальнейшее распространение содержимого, поскольку электронные письма легко пересылаются, сохраняются и распечатываются. Также, если электронная почта доступна на нескольких электронных устройствах, вероятность нежелательного воздействия возрастает. Устройства и электронные письма отправителя могут быть скомпрометированы, а получатели также подвержены взлому. [5]

Хотя электронная почта является полезным и распространённым средством общения в наши дни, существует слишком много способов, из-за которых конфиденциальная информация может стать доступна и использована злоумышленниками при отправке писем по электронной почте. Касаемо компаний, крайне важно оценить свою практику обмена файлами и документами и рассмотреть возможность инвестирования в сервис с максимальным обеспечением безопасной передачи файлов и писем.

Чтобы сохранить конфиденциальность учётной записи, следует придерживаться нескольких простых правил безопасного использования электронной почты (Email):

1. Использование надёжных паролей. Главное требование – следует делать пароль запоминаемым и сложным, чтобы его не могли методом подбора найти хакеры и мошенники. Никогда не использовать пароли, такие как «12345» или сочетание имени, фамилии с датой рождения. Пароль должен содержать заглавные и строчные буквы, знаки препинания, цифры.

2. Не должно быть одного пароля. Не использовать один и тот же пароль дважды. Это защитит другие учётные записи, даже если одна из них была успешно взломана хакером.

3. Избегать фишинга. *Фи́шинг* – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. Необходимо быть бдительным и внимательным к письмам от неизвестных и непроверенных людей.

4. Не торопиться нажимать. Не нажимать на ссылки или вложения в сообщениях со странным содержанием и от незнакомых отправителей. Таким образом можно загрузить вредоносное ПО на компьютер. В дополнение к установленным спам-фильтрам и антивирусным программам, нужно быть осторожным, чтобы не открывать вложения или переходы по ссылкам от неизвестных отправителей.

5. Скопировать важную информацию. Если есть важная информация, которую необходимо сохранить, можно перенести её в другую учётную запись, чтобы создать резервную копию.

6. Не использовать бесплатные сети Wi-Fi. Хакеры могут легко перехватить пароли в подобных местах, особенно если сеть не защищена паролем.

7. Сложный адрес электронной почты. Если создаётся новая учётная запись электронной почты, нужно придумать что-то уникальное. Чем сложнее адрес, тем сложнее хакерам его сгенерировать. [3]

Выбор почтового клиента

Почтовый клиент – это компьютерная программа, используемая для чтения и отправки электронных сообщений. Однако почтовый клиент – это не то же самое, что почтовый сервер; последний – это оборудование, которое транспортирует и хранит почту централизованно для многих пользователей электронной почты. Почтовый клиент, напротив, – это то, с чем взаимодействует пользователь.

Как правило, почтовый клиент загружает сообщения с сервера для локального использования (или для использования в браузере), загружает сообщения на сервер для доставки их получателям. Позволяет читать, организовывать и отвечать на сообщения, а также отправлять новые письма. Помимо текста электронной почты, почтовые клиенты также обрабатывают вложения, поэтому пользователи могут отправлять и получать компьютерные файлы (например, изображения, документы или электронные таблицы) по электронной почте.

Первый основной способ выбора почтового клиента – это использование клиента, который часто использует протоколы POP3, SMTP или IMAP для сбора почты непосредственно с сервера на компьютер или другое вычислительное устройство. Обычно это означает загрузку и установку программного обеспечения для почтового клиента. [2]

Второй основной способ – это использование облачных сервисов через веб-приложение. Это означает, что не нужно скачивать какое-либо программное обеспечение или даже иметь сервер для сбора электронной почты, так как всё хранится онлайн в веб-приложениях. Ещё лучше то, что по мере расширения онлайн-коммуникаций некоторые поставщики

электронной почты включают в свой сервис дополнительные инструменты совместной работы, например, видеоконференции.

Лучшие почтовые клиенты теперь не просто отправляют письма и управляют ими, а гораздо больше интегрируются в дополнительное программное обеспечение и приложения. Хотя почтовые клиенты могут потребовать немного больше работы для запуска, они также обеспечивают больший контроль над пользовательскими данными. Наиболее популярными почтовыми клиентами являются:

– Microsoft's Outlook;
– Gmail;
– Mozilla Thunderbird;
– The Bat!;
– Opera Mail.

Выбор правильного почтового клиента – это большое решение. Электронная почта по-прежнему является основным компонентом общения друг с другом. Поэтому важно использование почтового клиента, который имеет все необходимые функции. [6]

Поскольку злоумышленники воспользовались глобальным кризисом здравоохранения, безопасность электронной почты стала одной из основных проблем. Barracuda Networks сообщает, что с начала марта было обнаружено более 400000 случаев атак с использованием фишинга. Хотя цифры, безусловно, вызывают тревогу, хорошая новость заключается в том, что эти цифры могут резко упасть, если должным образом обучить сотрудников моделированию сценариев атак, особенно в то время, когда большинство сотрудников работают дистанционно.

Литература

1. Barracuda// [Электронный ресурс] – Режим доступа: https://www.barracuda.com/ - Дата доступа: 07.04.2021.

2. SendPulse. Что такое почтовый клиент? – Основы// [Электронный ресурс] – Режим доступа: https://sendpulse.by/support/glossary/email-client – Дата доступа: 03.04.2021.

3. SPY-SOFT.NET. 30 правил безопасности для защиты электронной почты// [Электронный ресурс] – Режим доступа: https://spy-soft.net/30-pravil-bezopasnosti-dlya-zashhity-elektronnoj-pochty/ – Дата доступа: 05.04.2021.

4. Techradar.pro. Best email clients of 2021: Free and paid apps and software// [Электронный ресурс] – Режим доступа: https://www.techradar.com/best/best-email-clients – Дата доступа: 01.04.2021.

5. Википедия. Свободная энциклопедия// [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/Фишинг – Дата доступа: 23.03.2021.

6. Мойрубль. Финансовый блог. Что такое логин и пароль, как их создать и где лучше хранить// [Электронный ресурс] – Режим доступа: https://myrouble.ru/chto-takoe-login-i-parol/ - Дата доступа: 25.03.2021.

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ, ПРИМЕНЯЕМЫЕ В ТАМОЖЕННЫХ ОРГАНАХ РБ

Муравицкая М.В., Хроколова В.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

В настоящее время обеспечение высокого уровня жизни, предотвращение легализации незаконно полученных денежных средств, провоза контрабанды, охрана целостности государства, его экономических интересов, производителей и потребителей, да и в целом, населения, является важнейшей задачей, возложенной на таможенные органы Республики Беларусь. Для ускорения, упрощения, улучшения качества проведения таможенных операций уже не один год идёт процесс автоматизации информационных систем и технологий, которыми пользуются таможенные органы в процессе своей работы.

Разработка, создание и использование информационных технологий, в том числе основанных на электронных способах обмена информацией, и средств их обеспечения осуществляются таможенными органами в соответствии с Таможенным кодексом. Внедрение информационных систем и информационных технологий с использованием средств вычислительной техники и связи осуществляется в соответствии со стандартами, действующими в Республике Беларусь, и международными стандартами.

На данный момент в Республике Беларусь активно используется такая информационная технология, как национальная автоматизированная система электронного декларирования (НАСЭД), которая представляет собой систему, осуществляющую информационную поддержку и автоматизацию таможенных операций, совершаемых должностными лицами таможенных органов и заинтересованными лицами (декларантами), с использованием письменных и электронных документов. Она является основой для обеспечения информационного взаимодействия таможенных