УДК 004.4 **Информационные технологии**

Убеев Валерий Геннадьевич, *специалист, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Россия, г. Санкт-Петербург*

КАК ОБЕСПЕЧИТЬ БЕЗОПАСНОСТЬ ПРИ ПОМОЩИ МЕНЕДЖЕРА ПАРОЛЕЙ

Аннотации: В статье описываются технологии, помогающие обеспечить пользователям и компаниям надёжные пароли, что такое менеджер паролей, как обезопаситься от злоумышленников занимающихся подбором паролей.

Ключевые слова: Менеджер паролей, кибератаки, аутентификация.

Annotations: The article describes technologies that help provide users and companies with strong passwords, what a password manager is, how to protect yourself from intruders engaged in password guessing.

Keywords: Password manager, cyber attacks, authentication.

В мире есть два типа компаний: те, которые взломаны преступниками, и те, которые взломаны и еще не знают об этом. Преступники беспощадны.

Сегодняшние кибератаки превратились в высокоуровневый шпионаж, осуществляемый надежными преступными организациями или государствами. В эпоху SaaS (software as a service) корпоративные данные с большей вероятностью будут храниться в облаке, а не в локальной среде. Используя сложное программное обеспечение для облачного сканирования, преступники могут взломать корпоративную систему в течение нескольких секунд после подключения к сети. И цена утечки данных может быть огромной.

В качестве важнейшей защиты от хакеров пароли использовались с момента появления Интернета, и я верю, что они будут использоваться и после

того, как я выйду на пенсию.

Тем не менее, большинство паролей не соответствуют минимальным требованиям безопасности, а количество компаний, не имеющих инструментов многофакторной аутентификации или корпоративных средств управления, ошеломляет.

Существуют независимые команды хакеров, миссия которых — «взломать что угодно, чтобы обезопасить все».

Количество взломов паролей растет, и подавляющее большинство взломов на предприятиях можно отнести к плохой безопасности паролей. Итак, как бизнес может защитить себя?

Строгая «гигиена» паролей в сочетании с корпоративным менеджером паролей, поддерживаемая политиками компании и многофакторной аутентификацией, снизит ваш риск. А в эпоху облачных технологий безопасность с нулевым доверием (Zero Trust) должна обеспечиваться для каждого соединения, каждого устройства, каждого пользователя, каждый раз.

Повторение паролей.

Почему слабые пароли так распространены? С увеличением количества онлайн-аккаунтов люди повторяют один и тот же, легко запоминающийся пароль для нескольких учетных записей. Эти слабые пароли могут быть легко взломаны, создавая уязвимости в системе безопасности, которые позволяют киберпреступникам получать доступ к данным компании, сотрудников и клиентов.

Независимо от того, были ли пароли украдены с помощью фишинга, вредоносных программ или прочих атак, они дают преступникам доступ к ценной информации о компании и/или личной информации. Эта украденная информация может быть продана на торговых площадках даркнета, где ее можно использовать для совершения атак.

Менеджер паролей может предотвращать проблемы до их возникновения, автоматизируя сброс паролей и предотвращая ненужные блокировки. При интеграции между системами и даже при наличии доступа за пределами бизнес-

активов сотрудников он может приносить реальную пользу для бизнеса. Тем не менее, лишь небольшая часть компаний покупает корпоративный менеджер паролей, ссылаясь на стоимость.

Я считаю, что инвестиционные затраты на менеджер паролей должны быть сопоставлены с потерями, связанными со взломом, и связанной с этим производительностью пользователей. Например, если пользователи не имеют доступа к своим компьютерам и у них нет доступа для выполнения двухфакторной аутентификации (2FA) — производительность сразу снижается, пока они звонят в службу поддержки и ждут, пока их разблокируют.

Начните с хорошей «гигиены» паролей.

Хороший пароль обеспечивает простой способ защиты от подавляющего большинства киберугроз. Давайте рассмотрим привычки в отношении паролей, которые могут свести к минимуму влияние слабости пароля и помочь повысить безопасность вашей организации.

Используйте 12-16 символьную строку цифр, специальные символы. прописные и строчные буквы, символы и слова, не входящие в словарь. Чтобы взломать такой пароль, потребовалось бы несколько лет.

Политика неповторения лучше всего. 52 процента всех интернет-пользователей признают, что используют один и тот же пароль для многих учетных записей. Одно повторение может поставить под угрозу безопасность вашего предприятия.

Часто меняйте пароли, особенно после успешной атаки. И не делитесь ими ни с кем и не записывайте их на стикерах.

Многоуровневая защита с двухфакторной (2FA) или многофакторной (MFA) аутентификацией, которая идеально сочетается со специальным приложением Authenticator, которое может генерировать уникальный и часто меняющийся код. Биометрическая аутентификация — отпечатки пальцев, сканирование сетчатки глаза — может повысить безопасность как часть MFA, но она не является надежной. Надежный пароль всегда будет важным компонентом биометрической аутентификации.

Причины использовать корпоративный менеджер паролей.

Частая смена способов аутентификации — один из лучших способов защиты от компрометации. Надежный менеджер паролей, такой как 1Password для предприятий, создает уникальные учетные данные для каждой учетной записи и надежно хранит их в хранилище, где отдельные лица, сотрудники или группы могут получить к ним доступ с помощью мастер-пароля. Вот девять причин, по которым менеджер паролей имеет смысл для бизнеса.

- Упростите перегрузку паролей: облачные менеджеры паролей обеспечивают удобный доступ к паролю на любом устройстве.
- Больше никаких слабых паролей: Длинные, сложные пароли, на взлом которых у хакеров ушли бы годы, легко генерируются менеджерами паролей.
- Мониторинг изменений паролей. Диспетчер паролей помогает поддерживать политику безопасности компании, отслеживая, как часто меняются пароли и соответствуют ли они политике компании.
- Сложнее взломать: менеджеры паролей затрудняют кражу личных данных преступниками, поскольку автоматически сгенерированные пароли не привязаны к личности пользователя и не содержат личных данных.
- Повысьте эффективность работы: ваша служба ИТ-поддержки тратит часы на решение запросов сотрудников на сброс пароля, что является пустой тратой бизнес-ресурсов. Менеджер паролей устраняет эти проблемы и повышает производительность ИТ-специалистов и конечных пользователей.
- Защита от фишинга и кражи личных данных: менеджер паролей не будет автоматически заполнять фишинговую форму, если пользователь щелкнет ее по ошибке. Он не только распознает ложное доменное имя, но также может предупредить об этом группу безопасности.
- Предотвращение утечки данных: генерируя уникальный пароль для каждого приложения, менеджер паролей устраняет эффект домино утечки данных при компрометации одной учетной записи.
- Встроенная двухфакторная аутентификация. Большинство

менеджеров паролей применяют двухфакторную аутентификацию или многофакторную аутентификацию для пользователей, прежде чем им будет разрешен доступ к корпоративному порталу или приложениям.

- Управление паролями в браузере: пользователи часто позволяют сохранять пароли в памяти браузера для автоматического заполнения при входе в систему. Это небезопасно для вашего бизнеса. Если устройство взломано, пароли могут быть украдены. При использовании менеджера паролей у пользователя должен быть один уникальный пароль, чтобы разблокировать хранилище.

Предпринимаются шаги к аутентификации без пароля. Например, Fast Identity Online 2 (FIDO2) обещает обеспечить бесперебойный и безопасный механизм онлайн-аутентификации. Однако внедрение потребует времени, и мы вряд ли увидим 100% внедрение. Что вы можете сделать в это время?

Есть шаги, которые организации могут предпринять, чтобы предотвратить и смягчить последствия взлома паролей. Предприятия, которые вкладывают средства в частое тестирование на проникновение, могут быстро обнаружить и усилить слабые пароли.

Правда в том, что люди будут продолжать забывать свои пароли, использовать небезопасные учетные данные и повторять их в разных учетных записях. Но вы не должны допускать, чтобы плохая «гигиена» паролей увеличивала риск вашей безопасности.

Zero Trust, поддерживаемый надежной политикой паролей, надежными инструментами управления паролями, обучением сотрудников передовым методам и регулярному тестированию на проникновение может защитить ваши корпоративные сети от киберпреступников, и похищающих учетные данные.

Библиографический список:

1. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код //Телекоммуникации. – 2013. – №. S7. – С. 27-29.

2. Волкогонов В. Н. и др. ПРИМЕНЕНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ДЛЯ ВЫПОЛНЕНИЯ АУТЕНТИФИКАЦИИ В СРЕДЕ ИНТЕРНЕТА ВЕЩЕЙ //Актуальные проблемы инфотелекоммуникаций в науке и образовании. – 2021. – С. 409-414.

3. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.

4. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.

5. Орлов Г. А., Красов А. В., Гельфанд А. М. Применение Big Data при анализе больших данных в компьютерных сетях //Наукоемкие технологии в космических исследованиях Земли. – 2020. – Т. 12. – №. 4. – С. 76-84.