ПАМЯТКА ПО КИБЕРБЕЗОПАСНОСТИ ДЛЯ КОНТРАГЕНТОВ

Кибербезопасность – обеспечение защищенности киберпространства, в котором функционирует бизнес, которое достигается применением набора средств, методик и принципов, направленных на противодействие угрозам в киберпространстве и минимизацию последствий от их реализации.

Выполнение простых правил кибербезопасности позволит создать общее безопасное киберпространство для достижения совместных целей и сделать сеть Интернет более безопасным местом.

Базовые правила кибербезопасности

1. Будьте осторожны с тем, какую информацию публикуете о себе, о других и о своей компании

Перед публикацией любой информации в сети Интернет ответьте на несколько вопросов:

- разглашает ли публикация Ваше текущее местоположение или, наоборот, говорит о Вашем отсутствии где-то на протяжении долгого времени?
- нарушает ли публикуемая информация соглашение о конфиденциальности, трудовой договор или иное соглашение, которое Вы или Ваша компания подписала?
- содержит ли публикация чужую личную информацию или бездоказательные публичные обвинения?

Если хотя бы на один из вопросов Вы ответили «Да», следует отказаться от публикации данной информации.

2. Понимайте, какие данные собирает Ваша компания, и убедитесь, что они защищены

Проведите инвентаризацию собираемых Вашей компанией данных и определите, какая информация является публичной, у каких данных средняя степень важности и какие наиболее критичны и конфиденциальны. Примите соответствующие меры для каждой категории: публичная не требует серьезных мер защиты, а информация высокой важности должна быть надежно защищена с использованием наиболее строгих правил доступа для сотрудников и контрагентов.

3. Используйте несколько факторов аутентификации

Аутентификация – это процесс подтверждения идентификационных данных (например, логина и пароля) путем сравнения предоставленных учетных данных с существующими сведениями об авторизованных пользователях перед получением доступа к системе или приложению. По возможности старайтесь использовать не только пароль, но и дополнительный фактор для аутентификации. Это может быть одноразовый код из СМС-сообщения, электронный сертификат или биометрический фактор (например, отпечаток пальца или распознавание лиц).

4. Установите SSL/TLS сертификат для Вашего сайта

SSL/TLS сертификат обеспечивает шифрование между браузером и сервером. Это обеспечивает защиту информации от злоумышленников. Также наличие SSL-сертификата позволяет пользователям убедиться, что сайт действительно принадлежит Вашей компании, а не является фишинговым.

5. Используйте надежные и уникальные пароли

Современные вычислительные мощности позволяют вычислить пароль из девяти букв в нижнем регистре за 10 секунд. Хороший пароль, обеспечивающий достаточную надежность, должен состоять не менее чем из 8 символов и содержать цифры, прописные и строчные буквы и символы. При этом лучше всего не использовать целые слова на любом языке, в том числе русские в английской раскладке клавиатуры. Использование уникальных паролей позволит сохранить безопасность остальных сервисов в случае, если пароль от одного из них будет скомпрометирован.

6. Обновляйте все программное обеспечение

Обновления программного обеспечения не только приносят в него новые функции или улучшают работу, но и закрывают обнаруженные уязвимости в программном коде. Регулярная установка обновлений позволяет обрести уверенность, что известные «дыры» в программном обеспечении закрыты «заплаткой»-«патчем». Если программное обеспечение обновить нельзя, внедрите и используйте компенсирующие меры.

7. Установите антивирусное программное обеспечение и регулярно обновляйте базы сигнатур

Ежедневно появляются сотни новых компьютерных вирусов и вредоносных программ. Избежать заражения позволит установка антивирусного программного обеспечения. Современные антивирусы позволяют распознать новый вирус по его поведению в системе, однако наиболее эффективным является регулярное обновление баз сигнатур – цифровых «отпечатков» вредоносного программного обеспечения.

8. Делайте резервные копии важных данных

Регулярное создание резервных копий гарантирует, что в случае потери данных их можно будет восстановить. При этом следует хранить резервные копии в нескольких местах и на нескольких носителях, чтобы в случае повреждения одной резервной копии была возможность использовать другую.

9. Установите и настройте межсетевой экран на границе Вашей сети

Межсетевой экран позволяет предотвратить несанкционированный доступ в корпоративную сеть. При этом важно установить набор правил для определения, какой трафик разрешен, а какой запрещен. Также не забывайте регулярно обновлять программное обеспечение самого межсетевого экрана (см. пункт 6).

Культура кибербезопасности для работников

10. Установите правила для использования собственных устройств на рабочем месте.

Использование личных устройств для работы сотрудников может повысить эффективность и продуктивность, но при этом открывает возможности для атаки, поскольку личные устройства могут быть не оснащены средствами защиты и использоваться для доступа к корпоративным ресурсам. Установите правила Bring Your Own Device для повышения осведомленности сотрудников по вопросам использования мобильных технологий и способов уменьшения риска такой атаки.

11. Создайте стратегию реагирования на инциденты безопасности

Гарантировать абсолютную безопасность невозможно при любых обстоятельствах, поэтому разработайте план действий в случае кибератаки на Ваши ресурсы. Это позволит гарантировать, что Вы сможете оперативно среагировать и предотвратите больший ущерб. Также Вы успеете предупредить прессу, регуляторов и контрагентов, если атака окажется сильнее, чем ожидалось. При этом следует убедиться, что назначены ответственные лица для реализации плана реагирования на инциденты, и они знают, что необходимо предпринять в соответствии с ним.

12. Обучите сотрудников работе с паролями

Обучите сотрудников правилам создания хороших паролей (см. пункт 5), а также правилам безопасной работы с паролями:

- не записывать пароль на бумажном носителе;
- не передавать пароли через онлайн-каналы коммуникации (мессенджеры, электронную почту и др.), если те не зашифрованы;
- для хранения сложных паролей использовать корпоративный менеджер паролей (встроенный в браузер не подходит);
- не использовать одни и те же пароли многократно для разных сервисов, а также не использовать корпоративные пароли в личных целях.

13. Убедитесь, что сотрудники знают и проверяют наличие HTTPS для используемых в работе сайтов

Обучите сотрудников проверять наличие знака HTTPS в адресной строке браузера (значок закрытого «замочка» или адресная строка, окрашенная в зеленый цвет) перед передачей любой информации на сайт. Если знак HTTPS отсутствует, туда нельзя передавать никакую информацию.

14. Используйте безопасные коммуникации по электронной почте и проведите тренинг по рискам фишинговых атак

Обучите сотрудников правилам безопасного использования электронной почты, в том числе правилам безопасной передачи конфиденциальной информации через электронную почту и правилам распознания фишингового письма, а также рассмотрите использования средств защиты электронной почты, включая средства шифрования сообщений, антивирусной защиты и проверки происхождения сообщений.

15. Руководители должны распространять культуру кибербезопасности

Высшее руководство компании не должно иметь существенных поблажек с точки зрения кибербезопасности, напротив, руководители должны первыми принять изменения в правилах корпоративной стратегии кибербезопасности. Если руководители покажут положительный пример, вся компания последует за ними.

16. Проводите киберучения для поддержания сотрудников в тонусе

Организуйте проведение киберучений по фишинговым или иным атакам для проверки готовности к ним сотрудников. Такие тесты следует проводить до и после тренингов по кибератакам, чтобы измерить эффект от проведенных занятий.

Противодействие злоумышленникам

17. Создайте группу быстрого реагирования

Создайте группу для реагирования на инциденты для помощи ответственным за соблюдение плана реагирования на инциденты. В группу быстрого реагирования может входить сотрудник, отвечающий за связи с общественностью, для публикации пресс-релизов, представитель отдела продаж для общения с клиентами и другие сотрудники в зависимости от размера и сферы деятельности компании.

18. Проведите анализ угроз

Анализ или моделирование угроз покажет потенциальные угрозы для ИТ-инфраструктуры, в том числе исходящие изнутри организации. Не стоит забывать, что такие угрозы могут представлять нынешние и бывшие сотрудники, подрядчики, вендоры, сторонние поставщики или партнеры.

19. Составьте инструкцию для быстрого реагирования

Убедитесь, что вы готовы быстро и эффективно отреагировать в случае кибератаки. Разошлите план сотрудникам компании и назначьте ответственного за его осуществление.

20. Обучите сотрудников правилам реагирования на инциденты

Знание о плане и о возможных типах атаки, а также детальные инструкции по реагированию на инциденты для конкретных должностей сотрудников поможет работникам помнить о своих обязанностях сохранять конфиденциальность и минимизировать риск утечки информации.

21. Делайте выводы из прошлых инцидентов и опыта других компаний

В случае, если инцидент все же произошел, после устранения последствий и возвращения к штатному режиму работы следует провести аудит. В рамках этого мероприятия необходимо проверить, что приняты необходимые меры, чтобы те же самые уязвимости не эксплуатировались снова, а также проверить актуальность действующего плана реагирования на инциденты и при необходимости внести изменения.

22. Всегда предполагайте наличие уязвимостей

Даже самая дорогая система защиты не может гарантировать абсолютную безопасность всех Ваших систем. Всегда следует предполагать появление новой уязвимости, актуальной для корпоративной сети, или прием нового сотрудника, через которого можно провести взлом.

Дополнительные меры кибербезопасности

23. Страховка для ИТ-инфраструктуры

Киберстрахование, или полис страхования киберрисков — страховой продукт для защиты бизнеса от рисков, связанных с пользованием интернетом, хранением и обработкой данных в электронном виде и пр. Благодаря киберстрахованию убытки компании из-за кибератаки обычно сводятся к минимуму, и финансовые последствия смягчаются.

24. Не забывайте про Интернет вещей

Интернет вещей – это сеть передачи данных между физическими объектами, оснащенными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней стороной.

При использовании Интернета вещей рекомендуется присваивать идентификаторы для всех вещей, что позволит проводить их аутентификацию при подключении к сети и гарантировать безопасную передачу данных между устройствами.

25. Убедитесь, что все системы доступны только через многофакторную аутентификацию или аутентификацию в нескольких точках

Помимо доступа к данным после прохождения многофакторной аутентификации (см. пункт 3), доступ к ИТ-инфраструктуре также должен быть ограничен. Это возможно осуществить через многофакторную аутентификацию, а также посредством аутентификации в нескольких точках, например, посредством прохождения аутентификации до загрузки операционной системы, в операционную систему и в конкретный сервис. Также необходимо учесть разграничение доступа на основе ролей и предоставление доступа к администрированию систем только определенным привилегированным пользователям.

26. Проводите тестирования на проникновение

Помимо злоумышленников, совершающих атаки с целью нарушить закон, украсть данные или причинить ущерб бизнесу, существуют «белые» хакеры. Они проводят тестирования ресурсов на проникновение с целью рассказать о существующих способах взлома систем, чтобы обеспечить их устранение и не допустить проникновение «черного» хакера.

27. Рассмотрите использование облачных сервисов

Облачные сервисы — полезный инструмент, особенно для малых и средних компаний, которые хотят отдать свои данные под защиту крупной компании. При регистрации у облачного провайдера важно убедиться, что вы все о нем знаете.

Где находятся дата-центры, где конкретно хранятся ваши данные и как можно получить доступ к ним.

Повышение устойчивости критичных систем

28. Убедитесь, что Ваша сеть сегментирована

Разбиение сети на сегменты позволит избежать получения злоумышленником контроля над всей сетью в случае проникновения в корпоративную сеть. Следует сегментировать системы по важности или по тому, насколько важна сеть для бизнеса.

29. Изучите нормы кибербезопасности для своей отрасли и старайтесь держаться выше них

В большинстве отраслей существует набор отечественных и международных стандартов и лучших практик по обеспечению кибербезопасности. Следует держаться выше норм, предъявляемых для Вашей отрасли и класса (уровня, категории) используемых систем.

30. Всегда продолжайте изучение новых технологий и средств защиты

Регулярно уделяйте время изучению последних лучших практик безопасности, вендоров и технологий. Будьте готовы к использованию новых инструментов и технологий для обеспечения безопасности Вашей инфраструктуры в сети Интернет.

В случае обнаружения инцидента кибербезопасности при взаимодействии с ООО «ТОТ» обратитесь по адресу электронной почты направления кибербезопасности kb@sberanalytics.ru.