ЦИФРОВОЙ МИР: БЕЗОПАСНОСТЬ В СЕТИ И ВНЕ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО

ЧТО ЗАЩИЩАЕМ

- Сервер - Данные сервера
- Электронные почты - Данные переписок (особенность пользовательских соглашений yandex.ru mail.ru)
- Сайт, старый сайт - Данные на сайте (что может случиться с заброшенным сайтом, почему важна антивирусная защита сайтов)
- Группы в социальных сетях - Данные социальных сетей
- Конференции в ZOOM – данные конференций
- Почта и облачные сервисы;
- IP-телефония
- Внутренние сети: LAN, Wi-Fi
- мобильные и т.п. устройства сотрудников (случаи с непонятными подключениями к сети...);
- кошельки/аккаунты платежных систем;
- Наши данные в других организациях, чужие данные в нашей организации

ЧТО ЗАЩИЩАЕМ

- различные базы данных: списки участников мероприятий, волонтеров...;

- CRM-системы: (Customer Relationship Management или Управление отношениями с клиентами) — это — прикладное программное обеспечение для организаций, предназначенное для автоматизации стратегий взаимодействия с заказчиками (клиентами), в частности, для повышения уровня продаж, оптимизации маркетинга и улучшения обслуживания клиентов путем сохранения информации о клиентах и истории взаимоотношений с ними, установления и улучшения бизнес-процессов и последующего анализа результатов. CRM-системой можно считать любой вариант контроля и учета, который поможет улучшить взаимодействие с клиентами:

Модели угроз для НКО

- Взлом почты, в т.ч. через фишинговые письма
- DDOS-атаки, перегрузка сайта огромным количеством трафика или путем отправки вредоносных запросов, что приводит к отказу или к сбою работы целевого ресурса.
- Взлом соцсетей (из-за спины отследили вводимый пароль)
- Некорректное использование соцсетей
- Воровство средств со счетов и из Яндекс-кошелька
- Утечка персональных данных о сотрудниках, жертвователях
- Взлом/угон сайтов НКО (десятки случаев с угоном доменов...);
- Технические проблемы (случаи с ошибками серверов...);
- сайты, которые заражают своих пользователей;
- человеческий фактор (случаи с простыми и явными паролями, открытыми почтовыми ящиками на компьютерах).

ПОТЕНЦИАЛЬНЫЕ ИСТОЧНИКИ УГРОЗ

- хакеры-экспериментаторы и прочие анонимусы
- коллеги (бывшие) (случаи с вредительством со стороны тех, кто имел доступ к данным, если имеют причины мстить, могут унести флэшку с паролями, оставить оформленные на себя домены, через них на НКО могут выйти злоумышленники и т.п.);
- что-то личное (случаи, когда у сотрудников есть личные проблемы, а их враг отыгрывается на организации);
- технические (случаи, когда сотрудники что-то сами неправильно делают...);
- административные (случаи, когда забывают заплатить за хостинг и т.п.);
- вероятности (случаи, когда влияют человеческие факторы и т.п., меняющееся со временем: запускаются новые проекты и т.п.).

ПУТИ ПРОНИКНОВЕНИЯ УГРОЗ

- *Вирусы, черви*
- В fb часто предлагают посмотреть видео, фото, в которых содержатся вирусы.
- когда пользователя подталкивают к какому-то действию (высылают ссылку для открытия), скопировать ссылку, проверить на вирусы на специальном сайте virustotal.com
- *Фишинг*
- Присылают акты сверки счетов и т.п., ник в коем случае не открывать без проверки и достоверности отправителя!
- *Гмэйл-фишинг*
- Если приходит письмо на бланке Gmail-а за подписью команды Gmail, не кликать.
- Если приходит письмо с google.com-адреса, что для вас «расшарен» такой-то файл, приходит ссылка, что нужно что-то подтвердить, нужно смотреть, есть ли gmail аккаунт.

ПУТИ ПРОНИКНОВЕНИЯ УГРОЗ

- *Через скайп*
- Могут выходить на вымогательство денег и т.п.
- При подозрительных письмах задавать вопросы типа «Где и при каких обстоятельствах мы познакомились?», использовать в скайпе двухфакторную авторизацию, сделать привязку к телефону.
- Запросы поверяем через другие программы связи: сервис virtual.com – загружаем файл или ссылку, чтобы проверить: переносим ссылку/файл, вставляем и узнаем.
- Присланные файлы бывают в формате, например, pdf, в которые при проверке на вирус обнаруживается несколько файлов. Если простят ввести простой пароль для открытия, то файл содержит вирус.
- **НЕЗНАКОМЫЕ ССЫЛКИ, НЕПОНЯТНЫЕ АТТАЧМЕНТЫ И Т.П. – НЕ ОТКРЫВАТЬ!**

БЕЗОПАСНОСТЬ САЙТА И ОСНОВНЫЕ УГРОЗЫ САЙТАМ НКО

- безопасность сайта зависит в т.ч. от программного обеспечения;
- нельзя защитить сайт от всех угроз;
- возможно нанять хороших специалистов, чтобы они анализировали каждый пакет трафика;
- чем больше вы, тем больше угрозы сайту;
- чем сложнее сайт, тем проще его сломать (убрать ненужные функции);
- делать бэкапы, распределенные бэкапы;
- повышать техническую грамотность персонала;
- проводить тренировки IT-специалистов по безопасности;
- проводить мониторинг сайта;
- проводить техническую чистку и переустановку сайта с нуля;
- если нет https, обязательно сделать (его отсутствие создает опасность для владельцев и пользователей);
- сложно оценить риски для сайта НКО (включают в себя: цену бесперебойной работы сайта, цену ущерба репутации от взлома сайта, оценку вероятности угроз для сайта).

ЧЕЛОВЕЧЕСКИЙ ФАКТОР, КАК «ТОНКОЕ МЕСТО»

- Каждый раз вводить пароль – это неудобно
- Шифровать диск – медленно
- Резервное копирование – долго и дорого
- Разработка и строгое соблюдение политики безопасности – сложно, лишний труд
- Что важнее удобства или безопасность?

ПОЭТОМУ, В ПЕРВУЮ ОЧЕРЕДЬ «РАБОТАЕМ» С ЛЮДЬМИ

ОЦЕНИТЕ ВСЕ «ЗА» И «ПРОТИВ»:

- Какова ценность/стоимость вашей информации?
- Каковы ресурсы («время-деньги») потраченные на ее получение?
- Сколько сил придется потратить на ее восстановление?
- Какие усилия придется потратить на нейтрализацию утечки информации?
- Кто из близких, коллег может пострадать из-за «потери» информации? Репутация?
- Какие меры безопасности приняты сейчас?
- Насколько меры безопасности сопоставимы с ценностью информации для вас?

Как предотвратить?

Правила

ШАГ 1. СФОРМИРУЙТЕ ПЕРЕЧЕНЬ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ И ДАННЫХ

- Нужно понимать специфику своей организации (какие активы и т.п.), что нужно защищать;
- Определите, какие сведения нужно контролировать, чтобы обеспечить информационную безопасность. составить список, какая есть информация: о клиентах, о партнерах (что можно, что нельзя давать и кому);
- Когда утвердите окончательный перечень, закрепите его внутренним нормативным документом — «Перечень информации, имеющей ограниченный доступ».
- В дополнение к перечню информации, создайте правила, регулирующие информационную безопасность. Например, «Политика безопасности».
- Составить план внедрения политики безопасности;

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

ШАГ 2. УСТАНОВИТЕ КРУГ ЛИЦ, КОТОРЫЕ ИМЕЮТ ДОПУСК К СВЕДЕНИЯМ

- Проанализируйте, кому из сотрудников компании для работы нужен доступ к конфиденциальным данным.
- Выделите тех, кому требуется постоянный допуск, а для остальных работников пропишите правила доступа к данной информации.

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

ШАГ 3. ПРОВЕДИТЕ ИНСТРУКТАЖ РАБОТНИКОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- В организации нужен хотя бы один человек, который понимает принципы безопасности;
- Чтобы поддерживать дисциплину, можно даже установить штрафы и взыскания за нарушение правил.
- Нужен человек-пример, у которого все настроено;
- Соблюдать постоянство – наметить ежемесячные/еженедельные проверки, у кого какие программы поставлены/работают;
- Внедрение: обобщенное выступление, собственный пример, специальное подталкивание (например, высылать информацию только в определенном формате

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

ШАГ 4. ИСПОЛЬЗУЙТЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ, КОТОРЫЕ ПОЗВОЛЯТ СПЕЦИАЛИСТАМ ПО БЕЗОПАСНОСТИ КОНТРОЛИРОВАТЬ СОТРУДНИКОВ

- Совет весьма спорный, но допустимый , когда сотрудник работает на корпоративном ноутбуке.
- Либо просто не давать в руки всех, кто работает, ценных конфиденциальных документов.
- Самые быстрые и простые меры, которые вы можете предпринять: Установите пароли для документов и папок сократите набор прав

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

ШАГ 5. КОНТРОЛИРУЙТЕ СМЕНУ ПАРОЛЕЙ И КЛЮЧЕЙ

- Чтобы усилить меры безопасности, периодически меняйте электронные ключи и пароли от учетной системы, электронной почты сотрудников.
- Если увольняете работника или меняете его обязанности, смените все пароли, к которым он имел доступ, и проконтролируйте, чтобы он сдал все электронные носители.

- Источник: https://www.fd.ru/news/48239-informatsionnaya-bezopasnost-pri-organizatsii-udalennoy-raboty

Как предотвратить?

Программы

Установить систему проверки всех процессов, выполняемых подключенным компьютером. Таким образом, можно будет остановить кибер-атаки, которые не используют вредоносные программы , а также сложные и неизвестные атаки, благодаря которым злоумышленники могут проникнуть в корпоративную сеть через компьютер сотрудника без его ведома.

Соединение между компьютером и корпоративной сетью всегда должно быть защищено с помощью VPN (виртуальной частной сети). Такая частная сеть позволяет создавать защищенную локальную сеть без необходимости физического подключения ее участников друг к другу.

Пароли, используемые для доступа к корпоративным службам, и пароли сотрудников в целом должны быть сложными и трудными для расшифровки.

Важно использовать многофакторную аутентификацию (MFA). Благодаря этой двойной системе проверки доступа, можно более эффективно защитить доступ к VPN, к логинам сотрудников для корпоративных порталов и ресурсов, к облачным приложениям. Она даже поможет соблюдать требования по защите данных.

Системы межсетевого экрана, будь то виртуальные или физические, являются первой линией защиты в корпоративной сетевой безопасности. Эти системы отслеживают входящий и исходящий трафик и принимают решение о блокировке или разрешении определенного трафика на основе набора ранее определенных политик безопасности

Службы мониторинга для сетей, приложений и пользователей, а также службы реагирования и устранения возможных сбоев также необходимы для мониторинга и обеспечения непрерывности работы при удаленной работе его сотрудников.

ЛАЙФ-ХАК:
МЕНЕДЖЕР (МАСТЕР) ПАРОЛЕЙ

- **Плагин Lastpass https://lastpass.com/ru/**
- **Хранилище паролей**

Возможности:

- Помнит все! ваши пароли
- Генерирует сложные пароли
- Вводит пароль за вас!
- !!! Запомнить один мастер-пароль!!!
- Но, если получить доступ, то можно получить доступ почти ко всему

ЛАЙФ-ХАК:
ДВУХФАКТОРНАЯ (ДВУХЭТАПНАЯ) АУТЕНТИФИКАЦИЯ

- Google https://www.google.ru/intl/ru/landing/2step/
- Справка https://support.google.com/accounts/answer/185839?hl=ru **Как настроить двухэтапную аутентификацию**
- Откройте настройки аккаунта.
- В разделе "Безопасность и вход" выберите Вход в аккаунт Google.
- Нажмите Двухэтапная аутентификация. Откроется страница настроек функции.
- Следуйте инструкциям, которые будут появляться на странице.
- Затем вы снова попадете в раздел настроек двухэтапной аутентификации. Обязательно проверьте параметры и укажите дополнительные номера телефона. При следующем входе в систему вы получите SMS с кодом подтверждения.

ПОЛИТИКА БЕЗОПАСНОСТИ

- *Образец*

- ***Меры предосторожности, обязательные для всех сотрудников***
- *(предполагаются дополнительные меры для отдельных сотрудников: бухгалтер, системный администратор, пресс-секретарь...)*

- Безопасность всего проекта безопасна настолько, насколько безопасно самое слабое звено. В связи с этим следует практиковать холистическую безопасность, т.е. охватывающую все аспекты цифровой безопасности.

- Требования распространяются на все рабочие компьютеры, ноутбуки и смартфоны, если с них происходит работа с организационными серверами/аккаунтами.

- Мы понимаем, что адаптация данных принципов требует серьезного изменения цифрового поведения. В связи с этим дается месяц для адаптации. Месяц считается со дня подписания данного документа.

- **1.1. Ваш компьютер**
- С помощью вашего компьютера вы имеете доступ к следующим объектам, играющим огромную важность для организации:
- Сайт организации.

1. Переписка с коллегами, включающая чувствительную административную и финансовую информацию.

- Правила работы:
- 1. Все пароли, используемые сотрудником организации для электронной почты, должны содержать цифры, большие и малые буквы алфавита, по возможности – знаки препинания. Рекомендуется использование парольных фраз (passphrase – более длинных и замысловатых сочетаний символов, имеющих смысл только для автора) вместо паролей.
- 2. Все операционные системы сотрудников организации с помощью системного администратора должны быть обновлены до самой последней версии не позднее 14 дней со дня публикации.

- 3. Запрещается подключаться к открытым (т.е. к таким, на которых не установлен пароль) Wi-Fi сетям без использования VPN (Open PN, Cloak или другого), а также не устанавливать самостоятельно никаких программ и приложений (только с помощью системного администратора).
- 4. Каждый сотрудник или системный администратор обязан включить полное дисковое шифрование на компьютерах, используемых для работы.
- 5. В случае хранения на персональном компьютере чувствительных материалов (такие как пароли доступа, финансовые и административные материалы, а также персональные данные третьих лиц), связанных с работой в организации, эти файлы должны храниться в запароленной и зашифрованной папке.
- 6. Каждый сотрудник организации обязан настроить и регулярно выполнять полный бекап своего рабочего компьютера. Бекапы должны быть зашифрованы. Возможна передача выполнения этой операции системному администратору.

- 7. На компьютере каждого сотрудника организации системный администратор обязан установить антивирус на свой компьютер с обязательной проверкой всех флешек.
- 8. Рекомендуется отказаться от подключения флешек, мобильных телефонов («Можно я тут подключу свой телефон, мне надо зарядить») третьих лиц. Внимательно следить за передвижениями посетителей офиса.
- **1.2. Ваша электронная почта, онлайн-документы и службы электронных сообщений**
- 1. Каждый сотрудник обязан ввести двухфакторную идентификацию в своей рабочей почте, используемой для переписки с коллегами (с помощью системного администратора).
- 2. Каждому сотруднику рекомендуется настроить двухфакторную идентификацию во всех используемых социальных сетях (при необходимости – с помощью системного администратора).

- 3. Каждый сотрудник должен создать себе PCP-ключ и прислать его коллегам. Рабочий компьютер сотрудника должен иметь программу, способную открывать PGP-зашифрованные письма (gpg-tools, enigmail+thunderbird) (с помощью системного администратора).
- 4. Использование PGP-шифрования обязательно в следующих случаях:
- a. Отправка персональной информации о себе или третьих лицах.
- b. Отправка паролей доступа к почте или иным сервисам.
- 5. Всем сотрудникам необходимо зарегистрироваться в приложении Signal (или другом подобном приложении) и соединиться с коллегами. Такое приложение – резервный канал для паролей и прочей конфиденциальной информации.
- 6. Все документы в Google Docs должны иметь закрытый режим. При расшаривании документов следует расшаривать только по конкретным электронным адресам.

Политику безопасности прочитал и принимаю

Дата Подпись

Чек лист безопасности

1.	Для удалённой работы используются защищенные каналы связи, например, при помощи VPN (Virtual Private Network)?	
2.	При подключении к инфраструктуре пользователь проходит двухфакторную аутентификацию (токены, одноразовые пароли)?	
3.	При удалённом подключении не используются личные устройства сотрудников?	
4.	На удалённых рабочих местах контролируются съемные носители, запрещен «прямой» доступ в сеть интернет?	
5.	При подключении к сети компании происходит проверка удалённых устройств на наличие антивируса и его актуальности и на наличие необходимых обновлений безопасности?	
6	Использование корпоративных сервисов разрешено только со специально сконфигурированных «джамп-узлов»: терминальных серверов, виртуальных рабочих столов (VDI)?	
7.	В ИТ-инфраструктуре компании выполнено сегментирование и настроены разграничения доступа, пользователи имеют минимальный для работы набор прав?	
8.	В ИТ-инфраструктуре компании определены и применяются политики информационной безопасности и аудита событий?	
9.	Обеспечивается ли постоянный мониторинг и реагирование на события безопасности для обнаружения и предотвращения компьютерных атак и инцидентов, до того момента, как они могут вызвать реальные негативные последствия для компании?	
10.	Выполняется ли контроль изменений состава ресурсов, для которых предоставлен удалённый доступ, анализ защищенности сетевого периметра и инфраструктуры, обнаружение и устранение уязвимостей и ошибок настройки	

БЕЗОПАСНОСТЬ МОЖЕТ СТОИТЬ ДЕШЕВО, НО ЗАПЛАТИТЬ ЗА НАРУШЕНИЕ ЕЕ ПРАВИЛ ПРИДЕТСЯ ДОРОГО

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» – ЭТО ПРОЦЕСС ОБЕСПЕЧЕНИЯ ДОСТУПНОСТИ, ЦЕЛОСТНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ ИНФОРМАЦИИ.