White Paper

Безопасная удаленная работа
Проблемы и решения

Содержание

Введение

Каждая организация должна быть готова обеспечить непрерывность и эффективность бизнеса. Важнейший компонент непрерывности- поддержка частичного или полного перехода на удаленную работу. Предприятия должны поддерживать безопасное удаленное подключение к корпоративной сети в условиях, когда системы не могут выдерживать возросшую нагрузку, большинство общедоступных, домашних сетей небезопасны, а личные устройства и IoT являются векторами хакерских атак.
Пандемия COVID-19 остро поставила вопрос об организации удаленной работы.

Переход на удаленную работу

Рост числа кибератак

Экстренный переход на удаленный режим стал причиной возникновения таких проблем, как:

- Дистанционный контроль и организация деятельности сотрудников;
- Необходимость наличия большого количества техники для обеспечения штата в домашних условиях;
- Информационная безопасность.

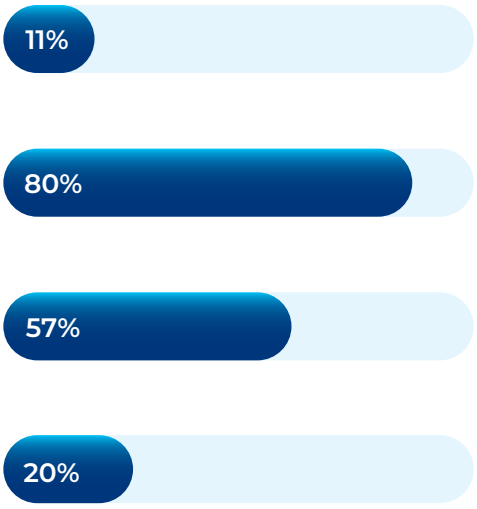
Большинство организаций быстро перешли формат work-from-home и еще не изменили свои методы обеспечения кибербезопасности. В то же время, киберпреступники нацеливаются на уязвимости, появившиеся в результате новой реальности удаленной работы.

Решения по обеспечению безопасности системы work-from-home актуальны не только в подобные исключительные периоды.

Статистика

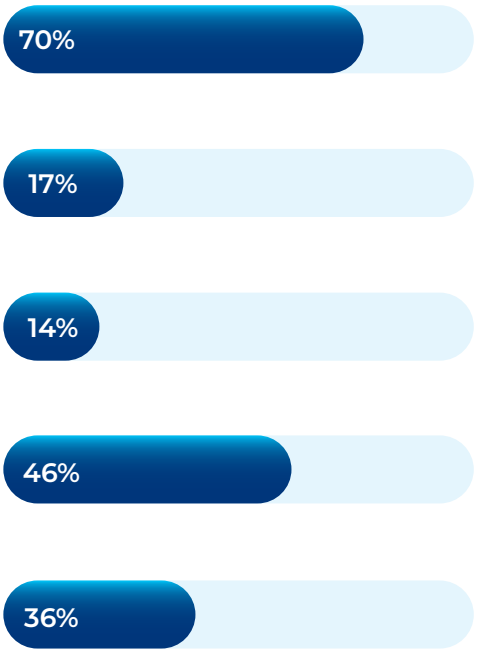
Positive Technologies представили результаты исследования:

- Только 11% респондентов отметили, что в их компании удаленный доступ организовали в связи с карантином;
- 80% респондентов рассказали, что в их компаниях часть сотрудников или все из них используют для работы домашние компьютеры или ноутбуки;
- 57% респондентов отметили, что не планируют менять способы организации удаленного доступа в ближайшее время;
- Каждая пятая компания вывела на периметр корпоративные порталы.



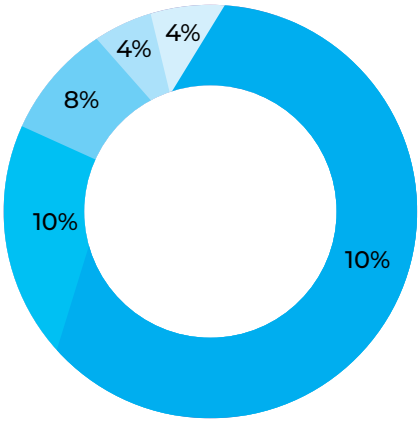
Osterman Research подвели итоги опроса, охватывающего средние и крупные предприятия разных стран: :

- 70% организаций сообщают, что нынешний кризис негативно отразился на их способности поддерживать нормальную работу;
- 17% опрошенных организаций сообщили, что кризис практически не повлиял на их операционную деятельность;
- 14% сообщили, что он фактически улучшил их операционную деятельность;
- 46 % опрошенных обеспокоены тем, что хакеры попытаются воспользоваться ситуацией, когда сотрудники работают на дому, тем самым увеличива угрозу кибератак;
- 36% беспокоятся, что сотрудники подвержены фишинговым атакам и опосаются, что будут ошибочно открыты электронные письма, содержащие вредоносное ПО.



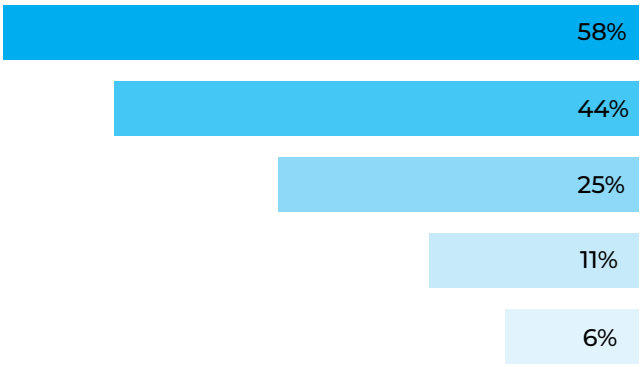
Group-IB провела опрос среди сотрудников более 100 российских и иностранных компаний об особенностях перехода на удаленную работу в их организациях во время COVID-19.

Работа из офиса vs. работа из дома



- Работают из дома
- Частично работают из офиса, частично из дома
- Работают из офиса
- На карантине или больничном
- Работа приостановлена

Механика организации удаленного доступа



Рабочий ноутбук с доступом к ИС и корпоративным файлам через VPN

Домашний компьютер с доступом к ИС и корпоративным файлам через VPN

Любой компьютер с настроенным удаленным рабочим столом

Рабочий ноутбук со свободным доступом к ИС и корпоративным файлам

Рабочий ноутбук доступ к файлам в облачном хранилище, без доступа к ИС

Какие департаменты переведены на удаленку

73%	61%	57%	56%	54%
ИТ/ИБ	Бухгалтерия	Коммерческий	Юридический	Маркетинг

Рост угроз безопасности

Мы наблюдаем увеличение атак с помощью вредоносного ПО, вирусов-шифровальщиков, фишинговых и DDoS-атак. С конца февраля 2020 года количество фишинговых атак возросло более чем на 600%.

Объектом нападений становятся госучреждения, финансовые организации, сектор здравоохранения, IT-компании, промышленные предприятия, профессиональные услуги и розничная торговля – киберпреступлениями затронуты все отрасли, и количество атак продолжает расти.

Финансовый ущерб

Убытки от них весьма значительны. В июне японский автопроизводитель Honda заявил, что программа-вымогатель поразила внутренние серверы компании, в том числе ее производственные системы, что вынудило ее приостановить производство некоторых автомобилей и мотоциклов.

Израильская финтех-компания Sapiens заплатила выкуп в размере 250 000 долларов в биткойнах после того, как хакеры пригрозили закрыть сеть компании. Компания считает, что атака произошла в марте или апреле, когда сотрудники начали работать из дома.

Типичная утечка данных для крупной компании приводит к потере от 10 до 99 миллионов записей и снижает стоимость компании на 7,27%. Для малого бизнеса утечка данных может иметь катастрофические последствия.

Угрозы кибербезопасности

1. Отсутствие системы обучения персонала основам кибербезопасности. Сотрудники, могут посещать со своих устройств сторонние сайты и приложения, а также открывать спам-письма.

2. Отсутствие политик и регламентов безопасности удаленной работы.

3. Отсутствие контроля над приложениями, пользователями и данными: неконтролируемые личные устройства, используемые для доступа к электронной почте, приложениям или данным, часто создают слепые зоны безопасности, увеличивая риск потери данных.

4. Отсутствие средств контроля безопасности для предотвращения НСД: домашние сети не обеспечивают такого уровня безопасности и контроля, как корпоративные сети.

5. Облако: стремительный переход к публичным облакам во время карантина повлёк за собой увеличение числа хакерских атак, которые были нацелены на конфиденциальные данные. Облачные ресурсы, доступ к которым был в значительной степени ограничен через корпоративные сети и средства контроля безопасности, оказались открыты для доступа из любого места и с любого устройства.

6. Угроза случайного раскрытия информации: удаленная работа, создала больше возможностей для ошибок, которые увеличивают риск непреднамеренной утечки данных.

7. Незащищённые мобильные устройства: злоумышленники находят новые способы заражения мобильных устройств, изобретают дополнительные методы обхода средств защиты и размещения вредоносных приложений в официальных магазинах приложений.

Устранение угроз: что нужно сделать

К минимальным требованиям относятся:

- Создание политик безопасной удаленной работы
- Обучение сотрудников
- Регулярные обновления
- Использование VPN
- Многофакторная аутентификация и политика нулевого доверия
- Защита конечных точек
- Шифрование данных
- Резервное копирование

Полный перечень дополнительно включает:

- Средства защиты периметра сети
- Мониторинг
- Управление мобильными устройствами (MDM)
- Сегментация сети
- Контроль утечки информации

1. Политика безопасной удаленной

Три компонента, которые необходимо рассмотреть при разработке политики безопасности удаленной работы, включают в себя сотрудников, технологии и процессы.

Сотрудники

Аспекты, которые необходимо предусмотреть при разработке политики:

- Какие роли имеют решающее значение для обеспечения непрерывности бизнеса, и какие из них могут быть полностью удаленными? Некоторые роли могут быть частично удаленными, поскольку они включают в себя функции, которые должны выполняться в офисе;
- Какие роли критичны для поддержания работы на объекте? Они могут включать в себя IT и безопасность, если у вас есть локальный дата-центр или операционный центр безопасности (SOC);
- Определите ранжирование доступа по ролям в соответствии с должностными обязанностями;
- Кто является ответственным за обеспечение кибербезопасности при удаленной работе? Опишите правила поведения, должностные обязанности и ответственность. Укажите контакты для связи;
- Какой уровень взаимодействия вы ожидаете от удаленных сотрудников? Будьте готовы к снижению производительности сотрудников, которые обычно не работаю удаленно. По крайней мере, первоначально;
- Ваши политики должны быть гибкими и в то же время соответствовать действующему законодательству.

Технологии

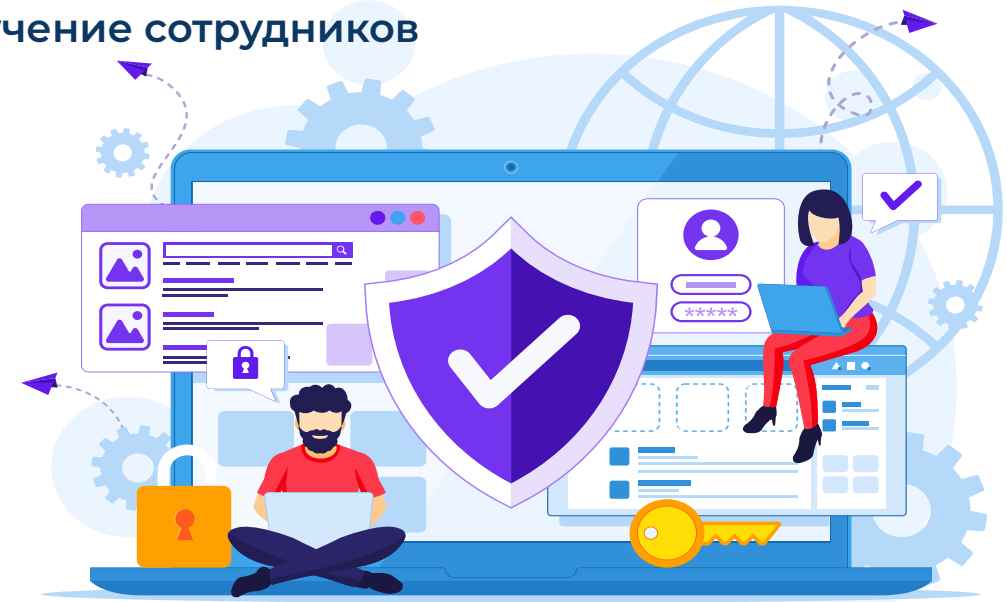
- Есть ли у вас безопасный способ подключения к корпоративной сети для удаленных сотрудников с помощью устройств, предоставляемых компанией? Виртуальная частная сеть (VPN) с многофакторной аутентификации - лучшая практика. Дополнительно, рассмотрите вопрос о том, чтобы не разрешать сплит-туннелирование VPN, чтобы свести к минимуму риск бэкдора;
- Будете ли вы разрешать удаленным сотрудникам использовать персональные устройства? Они представляют огромные риски, которые нужно предусмотреть. Какие шаги вы предпримете для минимизации вероятности инцидента с безопасностью?
- Разрешен ли удаленным сотрудникам доступ к рабочим файлам и электронной почте с персональных мобильных устройств?
- Какие инструменты необходимо предоставить для удаленной совместной работы, коммуникаций и управления проектами? Используют ли эти приложения защищенные протоколы и шифрование данных?
- Есть ли у вас средства для инвентаризации и классификации удаленных активов? Ноутбуки, которые покидают вашу сеть и подключаются к домашней среде, могут оставлять “слепые зоны”. По сути, если вы не видите его, то вы и не можете защититься. Это становится более серьезной проблемой по мере того, как все больше активов вашей компании покидают вашу доверенную сеть и подключаются к удаленным сетям.
- Какие технические решение буду использоваться для обеспечения бесперебойной работы компании?
- Какие технические решения будут использоваться для обеспечения режима защиты информации?
- Какие решения оптимальны и экономически выгодны?
- Опишите общие принципы работы средств защиты информации.

Процессы

- Какой у вас план обеспечения непрерывности бизнеса, если сотрудники не могут работать, выполняя критически важные функции в офисе или дома? Рассмотрите процедуры для таких сценариев, как запросы в службу поддержки ИТ, инциденты, связанные с кибербезопасностью, и экстренную связь между сотрудниками.
- С какими угрозами и рисками кибербезопасности может столкнуться ваша организация? Модель вероятных векторов атак. Профиль злоумышленников. Какой потенциальный ущерб может быть нанесен?
- Какие объекты информационной инфраструктуры наиболее значимы и требуют наибольшей защиты?
- Какие внешние и внутренние субъекты могут стать источниками угрозы информационной безопасности предприятия?
- Какая политика компании по работе через незащищенные каналы связи?
- Какие правила ввода новых ИТ-активов в строй?

- Какими принципами и стандартами руководствуется политика (ISO/IEC 27001-2005, ГОСТ и т.д.)? Какие требования к удаленной работе применимы к вашей организации? Какие нормативные-требования регуляторов должны соблюдаться?
- Какие действия должны предпринять сотрудники при инциденте, связанном с действиями хакеров, вирусными атаками или программами-шифровальщиками? Опишите порядок действий.
- Опишите в как будут проходить процессы резервного копирования, аварийные и восстановительные работы?
- Какие процедуры продолжат обеспечивать физическую безопасность? Вам все равно может потребоваться сохранение контроля физического доступа, камер видеонаблюдения, даже если вы активируете план по переводу всего штата на удаленную работу.

2. Обучение сотрудников



Подобно тому, как вы проводите обучение на реагирование в чрезвычайных ситуациях, необходимо проводить обучение и в области кибербезопасности. После того, как у вас будут разработаны политики удаленной работы проработайте сценарии реагирования, а также проведите дополнительный инструктаж по повышению осведомленности в вопросах кибергигиены.

Убедитесь, что лица, выполняющие критически важные функции, включая команды IT и безопасности, понимают политики и имеют возможность заранее задать вопросы и протестировать процедуры. Эта межфункциональная проверка позволяет убедиться, что политика, которая выглядит сильной на бумаге реализуется на практике.

Обучение каждого сотрудника компании мерам безопасности имеет решающее значение для защиты доступа к информации и критически важным системам. Подготовьте инструкцию по работе с данными компании, в которой отразите следующие аспекты:

- Осведомленность о видах фишинговых атак. Умение идентифицировать потенциально опасные письма;
- Усилить политику паролей и посоветовать сотрудникам не использовать личные пароли для корпоративных учетных записей. Рассмотреть вопрос об обязательном сбросе пароля/повторной аутентификации перед началом удаленной работы;
- Социальные сети. Посоветуйте сотрудникам не проверять социальные сети на корпоративных устройствах во время удаленной работы;
- Перекрестное обучение и подготовка ИТ-специалистов. Обеспечьте дополнительное обучение ИТ-специалистов и сотрудников службы безопасности при удаленной работе, чтобы они понимали, какие дополнительные риски им необходимо учитывать. Кроме того, вы можете провести перекрестное обучение сотрудников ИТ для выполнения основных функций обеспечения кибербезопасности, если другие варианты отсутствуют;
- Запрет на совместное использование рабочих компьютеров и других устройств. Когда сотрудники приносят домой рабочие устройства, эти устройства не должны использоваться совместно или использоваться кем-либо еще в доме. Это снизит риск несанкционированного или случайного доступа к защищенной информации компании;
- Информацию о компании нельзя загружать или сохранять на личных устройствах сотрудников или в облачных службах, включая флэш-накопители или облачные службы, такие как их личные учетные записи на Google, Яндекс. Диски или Dropbox;
- Все устройства сотрудников должны иметь последнюю версию ПО, которая устанавливается автоматически после перезагрузки устройства. Автоматическая загрузка обновлений не должна быть отключена;
- Защита домашнего роутера. Удаленные сотрудники должны убедиться, что установлен надежный пароль и обновления прошивки. Шифрование должно быть установлено на WPA2 или WPA3. Необходимо использовать самый высокий доступный уровень шифрования и отключить WPS;
- Если сотрудники пользуются личными устройствами, они должны установить на него средства антивирусной защиты;
- Использование общих сетей для работы с корпоративными данными должно быть под строжайшим запретом.

3. Регулярные обновления

Каждый информационный актив, будь то автоматизированное рабочее место или средство защиты, должен постоянно обновляться и поддерживаться в актуальном состоянии. Любая критическая система, которая устарела, является существенным риском безопасности.

4. VPN

Виртуальные частные сети (VPN) обеспечивают шифрование интернет-трафика. Если ваша организация уже использует VPN, убедитесь, что он охватывает все отделы и всех сотрудников. Если ваша компания не использует VPN, внедрение этого инструмента удаленной работы критически важно для безопасности ИТ-инфраструктуры вашего бизнеса.

5. Аутентификация и политика нулевого доверия

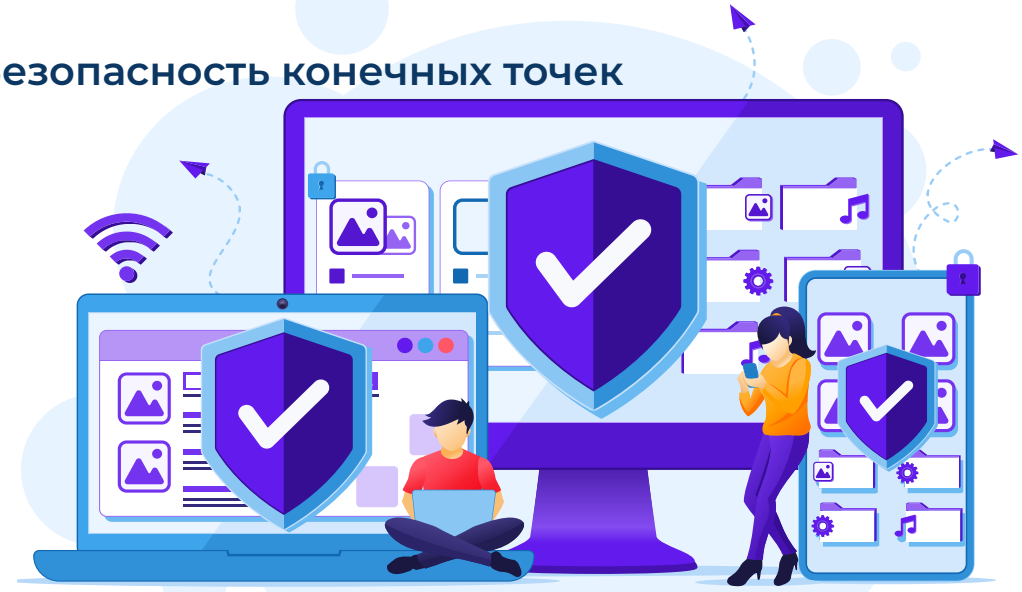
Скомпрометированные учетные записи часто служат точкой входа злоумышленников в сеть организации. Предприятия используют системы управления доступом для защиты своих информационных активов от растущих угроз кибербезопасности.

Сотрудники, работающие удаленно, должны использовать многофакторную аутентификацию (MFA) для доступа к сетям и критически важным приложениям. Внедрение многофакторной аутентификации добавляет несколько уровней безопасности доступа, выходя за рамки простого запроса имени пользователя и пароля. Пользователи должны предоставить дополнительные учетные данные, такие как код со смартфона, ответ на секретный вопрос и т.д.

Помимо доступа сотрудников, зачастую, организации настраивают доступ и для подрядчиков, поставщиков и партнеров. Различные типы пользователей требуют разного уровня доступа. Внедрение политики нулевого доверия подразумевает, что каждый сотрудник и компонент системы имеет лишь минимально необходимый доступ для выполнения своей работы и ничего более.

Контролируя доступ пользователей, компании могут устранить случаи нарушения политик безопасности, утечки личных данных и незаконного доступа к конфиденциальной информации. Решения по управлению доступом может предотвратить распространение скомпрометированных учетных данных и избежать несанкционированного проникновения в сеть организации. Проверенными и эффективными технологиями на рынке являются IDM, PIM и NAC решения.

6. Безопасность конечных точек



Рекомендуется обеспечить возможность работы через корпоративные устройства, которые прошли настройку с учетом всех требований безопасности. Это позволит вести деятельность с наличием актуальных обновлений для ПО и ОС под защитой антивирусных средств. Если же сотрудник использует личные устройства, то на каждом из них должно быть установлено антивирусное программное обеспечение.

Рабочие устройства, которые полностью исправлены и не содержат ошибок конфигурации, гораздо меньше рискуют быть скомпрометированными. Упреждающе идентифицируйте системы, подверженные риску, и исправляйте их как можно быстрее, особенно с учетом того, что они чаще находятся в сетях с минимальным или нулевым уровнем контроля безопасности.

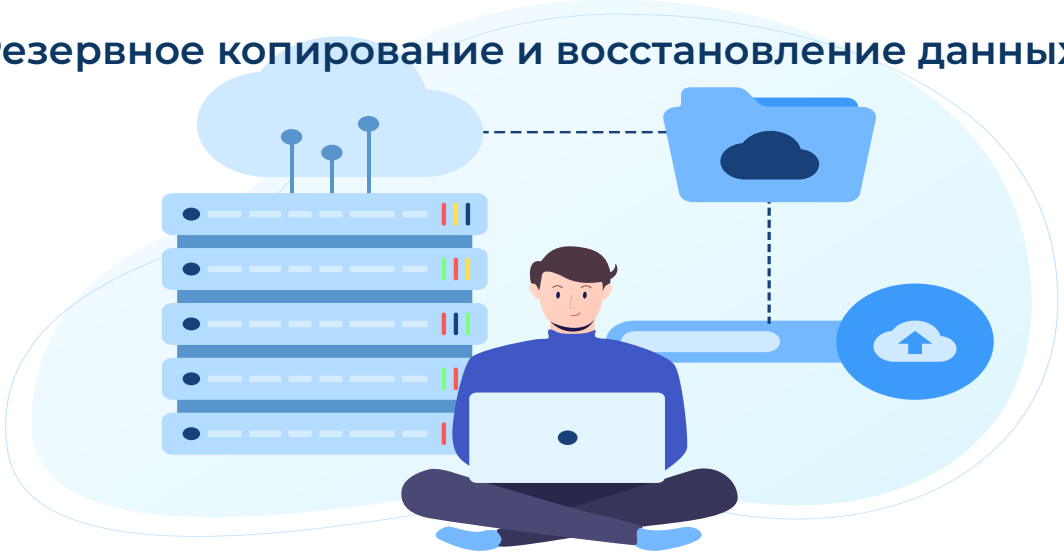
Агенты систем защиты конечных точек, установленные на удаленных устройствах, помогут провести полную инвентаризацию ваших информационных активов, чтобы лучше понимать области потенциального использования, и определить более четкую картину поверхности атак.

7. Шифрование данных

Используйте программное обеспечение для шифрования в целях защиты конфиденциальных данных, таких как персональные данные, информация о клиентах и партнерах, финансовые отчеты и т.д.

Все данные должны быть зашифрованы во время хранения или передачи. В случае нарушения целостности данных, кража критически важных файлов должна привести только к получению нечитаемой информации.

8. Резервное копирование и восстановление данных



Создайте комплексную систему резервного копирования и восстановления данных, которая будет включать любую конфиденциальную и критическую информацию. В случае атаки вируса-шифровальщика - восстановление предыдущей резервной копии может быть единственным решением.
Резервные копии должны быть протестированы и создаваться на регулярной основе. Если вы не можете восстановить резервную копию, вся система бесполезна. Бэкапы должны быть надежными и легко восстанавливаемыми.

9. Средства защиты периметра сети

Дополнительные меры безопасности, такие как межсетевые экраны нового поколения (NGFW), системы защита почтового сервера, система обнаружения и предотвращения вторжений (IDS/IPS) и системы обнаружения сетевых аномалий (NAD) помогут ИТ/ИБ отделу усилить безопасность периметра корпоративной сети.

10. Мониторинг

Чтобы предвидеть угрозы и принять превентивные меры, сотрудники должны понимать, как новые векторы атак изменяют среду угроз. Вы можете использовать решения для поиска и проверки новых вредоносных сигнатур, адаптированных к корпоративной специфике, или для проверки количества сканирований, нацеленных на корпоративную сеть.
Применяйте расширенный мониторинг в масштабах всей организации, особенно в отношении данных и конечных точек.

Чтобы расширить мониторинг, команды безопасности должны использовать и обновлять системы управления информацией и событиями безопасности (SIEM), а также настроить правила корреляций событий информационной безопасности.

Реализуйте круглосуточное покрытие и отслеживайте новые угрозы. Если у вас нет собственных ресурсов для круглосуточного мониторинга, рассмотрите возможность использования операционного центра безопасности (SOC), как поставщика услуг.

Организации, поддерживающие выполнение финансовых операций, должны рассмотреть возможность интеграции существующей antifraud системы с SOC для ускорения проверки и предотвращения мошеннических операций. Выявляйте группы пользователей с высоким риском. Некоторые пользователи, например, те, кто работает с персональной информацией или другими конфиденциальными данными, представляют больший риск, чем другие.

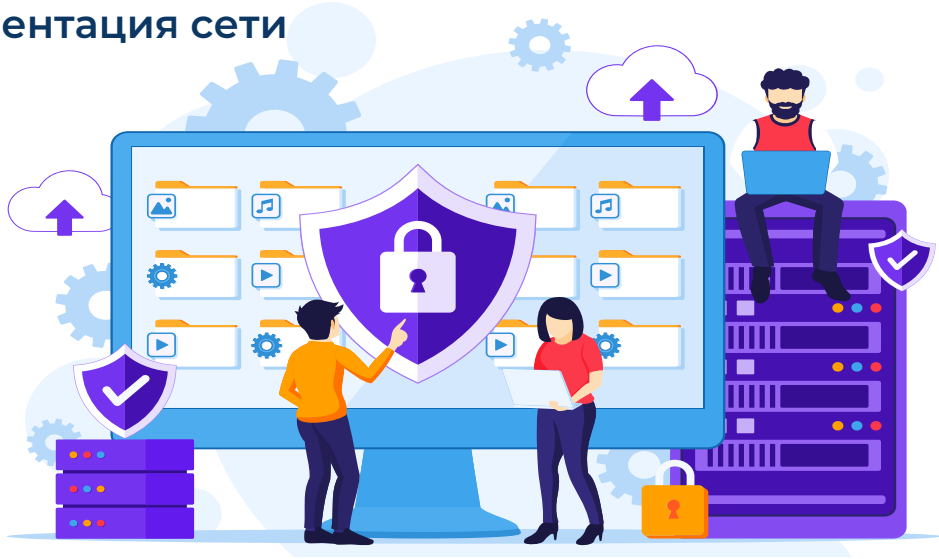
Пользователи с высоким риском должны быть идентифицированы и отслеживаться на предмет аномалий поведения (например, массовой загрузки корпоративных данных), которые могут указывать на нарушения безопасности.

Облачные службы, такие как Microsoft 365, Google Suite, AWS, Azure, являются инструментами, которые позволяют вашей удаленной рабочей силе быть более продуктивной. Мониторинг "облачной" среды на предмет угроз поможет защитить организацию и обеспечить непрерывность бизнеса даже в "облаке". Используйте интеллектуальную защиту от угроз: рассмотрите защиту от угроз нулевого дня, которая охватывает облачные среды, предотвращая утечку данных и потери от облачных вредоносных программ и программ-вымогателей.

11. Управление мобильными устройствами

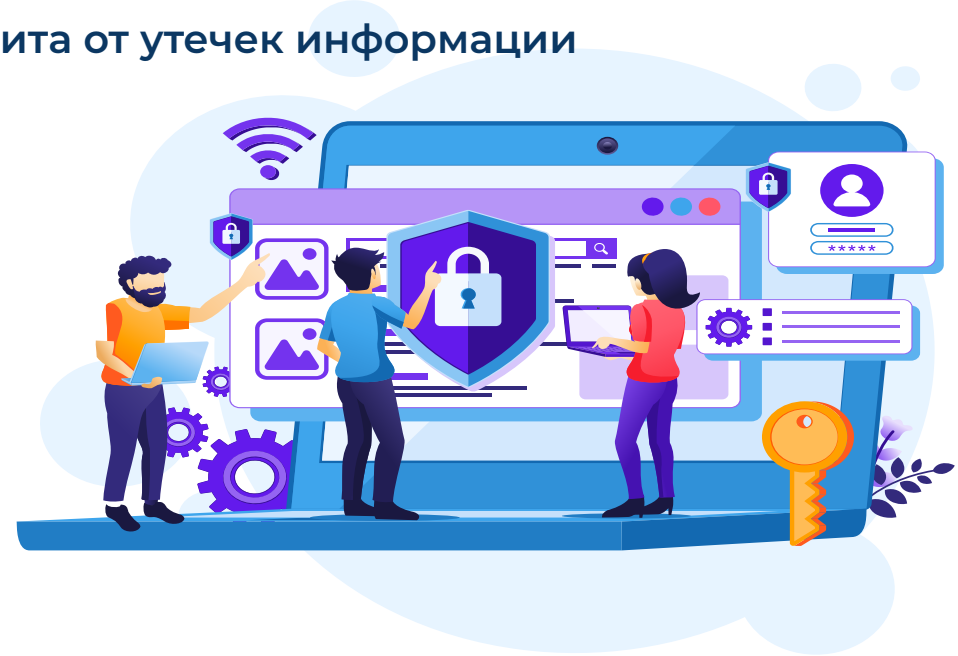
Если вы разрешаете сотрудникам получать доступ к ИТ-ресурсам компании с личного оборудования, воспользуйтесь стратегией «bring your own device» (BYOD). Разверните системы управления мобильными устройствами (MDM). Системы предоставляют администраторам инструменты и технологии для управления доступом, изменения роли пользователей, отслеживания действий, создания отчетов об этих действиях и обеспечения соблюдения политик безопасности.

12. Сегментация сети



Информационная среда организации должна быть разделена на отдельные защищенные сегменты. Это сделает ее более управляемой и повысит уровень защищенности.

13. Защита от утечек информации



Системы защиты от утечек информации Data Leak Prevention (DLP), предназначенны для защиты конфиденциальных данных от утечек, несанкционированного доступа и уничтожения. Системы данного класса анализируют и блокируют данные, передаваемые с помощью электронной почты, мессенджеров, Интернет-ресурсов и других источников.

DLP-системы позволяют контролировать рабочие места вне офиса и предотвращать утечки конфиденциальной информации из внутреннего периметра сети, даже если рабочая сеть и ее сегменты распределены географически.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

ООО «НТЦ ЕВРААС» может помочь вашей организации не только обеспечить безопасность информации и корпоративных ресурсов при переводе сотрудников на удаленную работу, но и внедрить комплексную программу кибербезопасности для вашей повседневной работы. Мы оказываем услуги услуги по проектированию и внедрению систем информационной безопасности предприятия различного уровня сложности.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru