ИНСТРУКЦИИ ДЛЯ СОВЕТА ДИРЕКТОРОВ: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

НАДЗОР

Являясь высшим звеном руководства организации, совет директоров несет полную ответственность за управление киберрисками и, следовательно, должен контролировать стратегию, политику и деятельность организации в этой области. В частности, совет директоров должен:

- Нести полную ответственность за контроль киберрисков и устойчивости как в качестве правления в полном составе, так и в случае делегирования надзора конкретному комитету совета директоров.
- Назначить одного корпоративного директора, как правило, главного директора по информационной безопасности, ответственным за отчетность о способности организации управлять киберустойчивостью и развитием в достижении целей устойчивости к угрозам кибербезопасности. Убедиться, что этот сотрудник имеет регулярный доступ к совету директоров, обладает достаточными полномочиями, имеет в распоряжении соответствующий коллектив, опыт и ресурсы для выполнения этих обязанностей.
- Ежегодно определять допустимость рисков организации; обеспечить согласованность с корпоративной стратегией и приемлемыми пределами рисков.
- Обеспечьте проведение ежегодного официального независимого анализа киберустойчивости организации.
- Обеспечить контроль над созданием, внедрением, тестированием и постоянным усовершенствованием планов киберустойчивости, обеспечением согласованности во всей организации, а также регулярностью отчетов перед советом директоров, предоставляемых главным директором по информационной безопасности или другим ответственным должностным лицом.
- Интегрировать процедуры киберустойчивости и оценки рисков в общую бизнес-стратегию организации, управление рисками, планирование бюджета и распределение ресурсов с целью полной интеграции киберрисков в общие операционные риски. Регулярно отслеживать риски в отношении третьих лиц.
- Периодически проверять собственную эффективность и учитывать независимые рекомендации по непрерывному усовершенствованию.

БУДЬТЕ В КУРСЕ

Эффективный контроль киберрисков зависит от коллектива участника и актуальной информации.

- Убедитесь, что все члены совета директоров имеют применимые и актуальные навыки и знания, позволяющие понимать связанные с киберугрозами риски.
- Регулярно консультируйтесь с руководством по текущим и будущим рискам в организации, соответствующим нормативным требованиям, а также отраслевым и социальным ориентирам для снижения приемлемых пределов риска. Также участвуйте в регулярных брифингах по последним разработкам в отношении ландшафта угроз и нормативно-правового регулирования, в совместном планировании и во встречах с коллегами и ведущими специалистами в области кибербезопасности, а также организуйте обмен опытом по вопросам управления и отчетности.
- Возложите на руководителей ответственность за предоставление количественно выраженной и доступно изложенной оценки киберрисков, угроз и событий в виде повестки дня во время заседаний совета директоров.
- Будьте всегда в курсе текущих системных проблем, например уязвимостей в цепи поставок, общих зависимостей и недостатка информации при обмене данными.

Основы управления киберрисками

Подтвердите, что вы можете утвердительно ответить на следующие вопросы:

1. Соответствует ли ваша организация **применимым законодательным и нормативным требованиям**?
2. Выполнила ли ваша организация **количественную оценку киберрисков и проверку финансовой устойчивости**?
3. Имеет ли ваша организация действующий **план по улучшению**, гарантирующий, что воздействие находится в приемлемых пределах рисков?
4. Регулярно ли совет **обсуждает лаконичную, четкую и действенную информацию касательно предоставляемой руководством устойчивости организации к угрозам кибербезопасности**?
5. Имеет ли ваша организация **планы реагирования на недавно протестированные инциденты**, в том числе на уровне совета директоров?
6. Являются ли **роли ключевых сотрудников, ответственных за управление киберрисками**, четкими и согласованным с тремя линиями защиты?
7. Получили ли вы **независимую аттестацию и гарантию** устойчивости вашей организации к киберрискам?

СОЗДАНИЕ АТМОСФЕРЫ

Помимо руководства высшего звена, совет должен определять и соблюдать основные ценности организации, культуру рисков и ожидания в отношении киберустойчивости.

- Поощряйте культуру, в которой сотрудники на всех уровнях осознают важность своих обязанностей по обеспечению киберустойчивости организации. Подавайте пример.
- Контролируйте роль руководства в формировании и поддержании в организации культуры рисков. Продвигайте, контролируйте и оценивайте культуру рисков, принимая во внимание влияние культуры на безопасность и надежность, а также при необходимости вносите необходимые корректировки.
- Четко объясните, что вы ожидаете от всех сотрудников добросовестного отношения и незамедлительного информирования обо всех случаях несоблюдения нормативных требований в организации или за ее пределами.

ИНСТРУКЦИИ ДЛЯ ГЕНЕРАЛЬНОГО ДИРЕКТОРА: ЛИДЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

УПРАВЛЕНИЕ

Кибербезопасность организации начинается и заканчивается на высшем уровне руководства. Генеральный директор и совет директоров должны понимать риски и нести полную ответственность за деятельность организации в области обеспечения кибербезопасности и подбора соответствующего персонала. Вы должны сделать следующее.

- Нанять директора по информационной безопасности (CISO) или, если ресурсы слишком ограничены, назначить сотрудника организации для выполнения этой функции.
- Сотрудничать с директором по информационной безопасности или другими техническими специалистами, чтобы разработать и обеспечить поддержку стратегии и структуры кибербезопасности, адаптированные к конкретным киберрискам организации, используя международные, национальные и отраслевые стандарты и руководящие принципы.
- Четко формулировать роли и обязанности персонала, обеспечивающего внедрение и управление кибербезопасностью организации.
  - Совместно с директором по информационной безопасности определять надлежащие роли в сфере кибербезопасности и права доступа для всех сотрудников.
  - Контролировать взаимодействие и сотрудничество с целью обеспечения целостности процесса управления кибербезопасностью, особенно если обязанности по обеспечению кибербезопасности передаются нескольким сотрудникам или подразделениям внутри организации (например, при наличии отдельных вертикалей управления информационной безопасностью, рисками и технологиями).
- Убедиться, что директор по информационной безопасности имеет четкую прямую линию коммуникации для своевременного уведомления вас и совета директоров об угрозах.
- Приглашать директора по информационной безопасности или другого технического специалиста для регулярного информирования высшего руководства.
- Обеспечивать единообразие политик, стандартов, механизмов принудительного исполнения и процедур обеспечения безопасности организации во всех подразделениях и направлениях деятельности.

ОЦЕНКА РИСКОВ И УПРАВЛЕНИЕ ИМИ

Обеспечение высокого уровня осведомленности о кибербезопасности и готовности к работе зависит от непрерывного анализа рисков. Для повышения уровня кибербезопасности организации сделайте следующее.

- Установите приоритет оценки рисков и управления рисками кибербезопасности в рамках более широкого процесса управления рисками в организации. Организуйте сотрудничество с директором по информационной безопасности или другим техническим специалистом по плану проведения оценки рисков, предусматривающему:
  - описание активов организации и различных уровней их зависимостей от технологических ресурсов;
  - оценку зрелости организации и неотъемлемых рисков, связанных с зависимостями ее активов от технологических ресурсов;
  - определение желаемого состояния зрелости организации;
  - анализ приоритетных областей для обеспечения кибербезопасности в организации;
  - выявление несоответствий между текущим состоянием и желаемым целевым состоянием кибербезопасности;
  - реализацию планов для достижения и поддержания зрелости;
  - оценка и выделение средств для инвестирования в безопасность и устранения существующих пробелов;
  - постоянную переоценку зрелости кибербезопасности организации, рисков и целей;
  - рассмотрение проведения проверки на проникновение третьих лиц или с привлечением «красной команды»,
  - рассмотрение возможности принятия защитных мер, таких как приобретение киберстраховки.
- Руководите работой сотрудников во время процесса оценки рисков, чтобы обеспечить своевременное реагирование по всей организации.
- Обеспечьте анализ и отчетность по результатам оценки рисков к рассмотрению исполнительным руководством, в том числе ключевыми заинтересованными сторонами и советом директоров.
- Контролируйте любые изменения, необходимые для поддержания или повышения готовности вашей организации к обеспечению готовности систем кибербезопасности, в том числе соответствующее выделение средств, гарантируя, что любые меры по улучшению систем кибербезопасности соотносятся с рисками и доступны для вашей организации.
- Контролируйте текущий мониторинг, который должен обеспечивать быстрое реагирование и гибкость в отношении возникающих киберрисков.

ОРГАНИЗАЦИОННАЯ КУЛЬТУРА

Кибербезопасность организации не является единовременным процессом или ответственностью нескольких сотрудников. Этот фактор необходимо учитывать во всех деловых решениях и операциях, а практика должна поддерживаться всеми сотрудниками. Поощряйте непрерывное и целостное обеспечение кибербезопасности в организации:

- Начните с обсуждения вопросов кибербезопасности с руководством и регулярно общайтесь с персоналом, отвечающим за управление киберрисками.
- Сделайте обучение принципам кибербезопасности частью процесса адаптации сотрудников и убедитесь, что все сотрудники осведомлены и подписали документы, подтверждающие соблюдение политик кибербезопасности организации, а также что ИТ-отдел или другой технический персонал провели их обучение передовым практикам.
- Проводите периодические тренинги по кибербезопасности для всех сотрудников в отношении их краткосрочных и долгосрочных обязательств.
- Убедитесь, что вопросы кибербезопасности всегда учитываются при оценке организацией потенциальных поставщиков и передаче данных третьим сторонам.

- Интегрируйте оценку кибербезопасности организации при рассмотрении возможности слияний и поглощений.
- Ежегодно пересматривайте политики кибербезопасности организации.
- Поощряйте добровольный обмен информацией об угрозах кибербезопасности и инцидентах в пределах организации и с доверенными партнерами.
- Содействуйте внедрению инноваций, которые изначально включают в себя вопросы безопасности и планирование.

ИНСТРУКЦИИ ДЛЯ ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ОРГАНИЗАЦИИ

ПРЕДОТВРАЩЕНИЕ УЩЕРБА ОТ ИСПОЛЬЗОВАНИЯ ВРЕДОНОСНОГО ПО

- Активируйте брандмауэр и установите списки контроля доступа (ACL) для создания буферной зоны между вашей сетью и Интернетом. Ограничьте доступ за счет внедрения списка разрешенных приложений, а не «черного списка» определенных IP-адресов или сервисов.
- Используйте антивирусное ПО и антишпионские программы на всех компьютерах и ноутбуках. Для защиты рассредоточенных трудовых ресурсов убедитесь, что инструменты для обеспечения безопасности могут эффективно работать в среде «работа из дома».
- Вносите исправления во все ПО и встроенное ПО, своевременно применяя последние предоставляемые разработчиками и поставщиками обновления ПО. По возможности активируйте функцию автоматического обновления.
- Убедитесь, что права на установку новых программ имеются только у ИТ-персонала с правами администратора.
- Обеспечьте ведение и мониторинг журналов активности аппаратным или программным обеспечением для защиты или обнаружения. Обеспечьте защиту журналов с помощью паролей и шифрования.
- Обеспечьте синхронизацию времени на всех хостах. Если время на устройствах организации будет несогласованным, то корреляцию событий в случае инцидента будет выполнить гораздо сложнее.
- Обеспечьте контроль доступа к съемным носителям, таким как SD-карты и USB-накопители. Вместо этого, поощряйте передачу сотрудниками файлов по электронной почте или через облачные хранилища. Информируйте сотрудников о рисках использования USB-накопителей из внешних источников или передачи их USB-накопителей другим лицам.
- Выполните настройку безопасности электронной почты и фильтров спама в сервисах электронной почты.
- Обеспечьте защиту всех страниц на общедоступных веб-сайтах с помощью шифрования и других доступных инструментов.
- Рассмотрите возможность найма службы проверки на проникновение для оценки безопасности активов и систем организации.

Разработка программы обеспечения информационной безопасности на основе рисков

1. Определите типы информации, которую хранит и использует организация

- Перечислите все типы информации, хранящейся или используемой в вашей организации (например, имена клиентов и электронная почта).

2. Определите ценность информации

- Задайте ключевые вопросы для каждого типа информации:
  - Что произойдет, если эта информация будет обнародована?
  - Что произойдет с моим бизнесом, если эта информация окажется неверной, например, если будет нарушена целостность данных?
  - Что произойдет с моим бизнесом, если я или мои клиенты не смогут получить доступ к этой информации?

3. Обеспечьте материальные средства

- Определите, какая технология вступает в контакт с определенной вами информацией. Это может быть аппаратное обеспечение (например, компьютеры) и программные приложения (например, электронная почта в браузере). Укажите марку, модель, серийные номера и другие идентификаторы. Отслеживайте, где находится каждый продукт. Для программного обеспечения определите, на какие машины оно было загружено. Поймите, как эти материальные средства могут перемещаться и разворачиваться в случае быстрого и/или массового развертывания работы из дома.
- При необходимости используйте технологические средства вне вашего бизнеса (например, «облачные хранилища») и любые имеющиеся инструменты защиты, например, брандмауэры.

4. Выработайте понимание угроз и уязвимостей

- Регулярно проверяйте, какие угрозы и уязвимости могут возникнуть в финансовом секторе и оценивайте вероятность их распространения на вас. (Информацию можно найти в национальных центрах CERT, FS-ISAC, местном подразделении InfraGard и других организациях.)
- Не реже одного раза в месяц проводите сканирование или анализ уязвимостей.
- Разработайте план защиты от внутренних угроз, включая оценку рисков на уровне предприятия и строгий контроль доступа.

ОБУЧЕНИЕ СОТРУДНИКОВ

- Проводите обязательные курсы обучения по кибербезопасности во время адаптации новых сотрудников и через регулярные промежутки времени для всех текущих сотрудников (не реже одного раза в год). Требуйте от сотрудников:
  - использовать надежные пароли для всех профессиональных устройств и учетных записей, а также аналогичным образом защищать личные устройства и использовать диспетчер паролей;
  - регулярно обновлять операционные системы, программное обеспечение и приложения на всех устройствах, включая домашнюю ИТ-инфраструктуру;
  - использовать двухфакторную аутентификацию для всех учетных записей;
  - хранить данные учетных записей и карт доступа в надежном месте и блокировать оставленные без присмотра устройства;
  - не обмениваться учетными данными или другой конфиденциальной информацией посредством незашифрованных электронных писем или других открытых сообщений;
  - не открывать вложения сразу же при получении и не переходить по ссылкам в нежелательных или подозрительных электронных письмах;
  - проверять достоверность подозрительных электронных писем или всплывающих окон перед предоставлением личной информации и обращать особое внимание на адрес электронной почты;
  - сообщать о любых потенциальных внутренних или внешних инцидентах в области безопасности, угрозах или неправильном обращении с данными или устройствами техническим специалистам организации и/или высшему руководству.
- Регулярно проверяйте осведомленность сотрудников посредством симуляции таких проблем, имитируя рассылку фишинговых электронных писем с фиктивных учетных записей. Используйте любые неудачи в качестве возможностей для обучения, а не наказания.

ЗАЩИТА ДАННЫХ

- Выполняйте регулярное резервное копирование важных данных (например, документов, электронных писем, календарей) и проверяйте возможность их восстановления. Рассмотрите возможность резервного копирования данных в облачное хранилище.
- Убедитесь, что устройство, содержащее резервную копию, не остается постоянно подключенным к содержащему оригинал устройству ни физически, ни по локальной сети.
- Установите стабилизаторы напряжения, используйте генераторы и убедитесь, что все компьютеры и критические сетевые устройства подключены к источникам бесперебойного питания.
- Используйте решения для управления мобильными устройствами (MDM).

5. Разработайте политику кибербезопасности

- Организуйте работу с высшим руководством организации, чтобы создать и обеспечить поддержку стратегии кибербезопасности, адаптированную к указанным рискам, используя международные, национальные и отраслевые стандарты и руководящие принципы. Такие руководящие принципы, как инфраструктура Национального института по стандартизации и технологии (NIST), инструмент оценки кибербезопасности FFIEC и стандарт ISO 27001, предоставляют шаблоны для создания и улучшения таких политик.
- Уведомите всех сотрудников о политике и попросите их подписать документы, подтверждающие их роль в постоянном обеспечении кибербезопасности в вашей организации в соответствии с положениями политики. В их числе должен быть четкий и хорошо понятный протокол «работы из дома».

БЕЗОПАСНОСТЬ УСТРОЙСТВ

- Включите ПИН-код и защиту паролем для мобильных устройств. Настройте устройства так, чтобы в случае утери или кражи с них можно было удаленно стереть данные или заблокировать.
- Своевременно обновляйте устройства (и все установленные приложения), по возможности используя функцию автоматического обновления.
- При отправке конфиденциальных данных не подключайтесь к общедоступным точкам доступа Wi-Fi, а используйте сотовые соединения (включая проводное соединение и беспроводные модемы) или используйте VPN.
- Замените устройства, которые больше не поддерживаются производителями, на более современные альтернативы.
- Разработайте процедуры отчетности о потерянном или украденном оборудовании.

ИСПОЛЬЗОВАНИЕ ПАРОЛЕЙ

- Убедитесь, что на всех компьютерах используются продукты шифрования, для загрузки которых требуется пароль. Включите защиту с помощью паролей или ПИН-кодов для мобильных устройств.
- Используйте надежные пароли, избегайте предсказуемых паролей (например, passw0rd) и личных идентификаторов (таких как имена родственников и домашних животных). Проследите, чтобы все сотрудники соблюдали эти правила.
- По возможности используйте двухфакторную аутентификацию (2FA).
- Измените пароли, установленные производителем по умолчанию на всех устройствах, включая сетевые устройства и устройства «Интернета вещей», до их передачи персоналу.
- Убедитесь, что сотрудники могут быстро изменить свои пароли. Вы также можете потребовать, чтобы сотрудники регулярно меняли свои пароли (например, ежеквартально, раз в полгода или ежегодно).
- Рассмотрите возможность использования диспетчера паролей. Если он уже используется, то убедитесь в надежности «основного» пароля (который обеспечивает доступ ко всем остальным паролям).

УПРАВЛЕНИЕ РАЗРЕШЕНИЯМИ

- Убедитесь, что все сотрудники имеют уникальные, идентифицируемые учетные записи, проходящие проверку при каждом доступе к системам.
- Предоставляйте административные полномочия только доверенным ИТ-сотрудникам и ключевым сотрудникам и аннулируйте права администратора на рабочих станциях для стандартных пользователей.
- Предоставляйте сотрудникам доступ к конкретным системам обработки данных только в случае необходимости для работы и убедитесь, что они не могут устанавливать ПО без разрешения.
- Контролируйте физический доступ к компьютерам и создавайте учетные записи для каждого сотрудника.
- Определите четкие параметры доступа для сотрудников и администраторов, работающих удаленно.

ЗАЩИТА СЕТЕЙ И УСТРОЙСТВ WI-FI

- Убедитесь, что Wi-Fi на рабочем месте надежно защищен и зашифрован с помощью WPA2. Маршрутизаторы часто поставляются с выключенным шифрованием, поэтому обязательно включите его. Пароль защищает доступ к маршрутизатору и обеспечивает обновление пароля из предустановленного значения по умолчанию. Отключите все функции удаленного управления.
- Настройте беспроводную точку доступа или маршрутизатор, чтобы он не передавал сетевое имя, известное как идентификатор набора служб (SSID).
- Ограничьте доступ к сети Wi-Fi, разрешая доступ только устройствам с определенными адресами контроля доступа к сети. Настройте отдельную общедоступную сеть Wi-Fi для клиентов.
- Активируйте вход через протокол динамической конфигурации хоста (DHCP) на сетевом устройстве, чтобы обеспечить простое отслеживание всех входящих в сеть устройств.
- После настройки маршрутизатора выйдите из системы как администратор.
- Регулярно обновляйте ПО маршрутизатора. Зарегистрируйте маршрутизатор на сайте производителя и подпишитесь на получение обновлений, чтобы своевременно узнавать об их появлении.

ПРЕДОТВРАЩЕНИЕ ФИШИНГОВЫХ АТАК

- Убедитесь, что персонал не просматривает веб-страницы или не проверяет электронную почту на серверах или с учетной записи с правами администратора.
- Настройте веб-фильтр и фильтр электронной почты. Рассмотрите возможность запрета посещения сотрудниками веб-сайтов, которые обычно связаны с угрозами кибербезопасности.
- Обучайте сотрудников способам проверки наличия явных признаков фишинга, таких как орфографические и грамматические ошибки, а также низкокачественные версии узнаваемых логотипов. Выглядит ли адрес электронной почты отправителя законным?
- Выполняйте сканирование на наличие вредоносных программ и изменение паролей в ближайшее время после появления подозрения об атаке. Не наказывайте сотрудников, если они стали жертвой фишинговой атаки (это приведет к тому, что в будущем они могут не сообщить вам о таком происшествии).

ИНСТРУКЦИИ ДЛЯ ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА КЛИЕНТОВ

УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ

- Требуйте, чтобы для входа в ваши сервисы клиенты использовали надежные идентификаторы пользователей и пароли. Посоветуйте им не использовать пароль, который уже используется для других учетных записей.
- Для проверки реальных клиентов и снижения возможности мошенничества используйте мгновенную верификацию, проверку в реальном времени, пробную проверку вклада, проверку личности и/или ответы на личные вопросы.
- Предлагайте, а лучше — требуйте от клиентов прохождения двухфакторной аутентификации при входе в ваши сервисы.
- Регулярно проверяйте учетные записи пользователей на наличие признаков мошенничества.

ЗАЩИТА ДАННЫХ

- Подумайте о том, какие данные клиентов организация должна собирать для предоставления своих услуг, и соблюдайте осторожность при сборе дополнительных данных клиентов.
- Разработайте и распространите политики хранения данных. Ликвидируйте данные клиентов, которые больше не будут использоваться.
- Обеспечьте шифрование передаваемых и неиспользуемых данных клиентов.
- Внедрите политики безопасности данных, чтобы четко обозначить разрешенные и запрещенные методы передачи данных и укажите допустимые процедуры для всех сотрудников при работе с данными клиентов. Убедитесь, что эти политики задокументированы, доведены до сведения всех сотрудников и периодически пересматриваются и обновляются.

ЗАЩИТА ОБЩЕДОСТУПНЫХ ВЕБ-ПРИЛОЖЕНИЙ

- Обеспечьте внедрение протокола HTTPS в общедоступных веб-приложениях организации и перенаправляйте весь HTTP-трафик по протоколу HTTPS.
- Используйте политику защиты содержимого на ваших веб-сайтах для предотвращения атак, связанных с межсайтовым скриптингом, кликджекингом и другими методами внедрения кода.
- Активируйте закрепление публичного ключа на своих веб-сайтах для предотвращения атаки с применением технологии «злоумышленник в середине».
- Убедитесь, что в общедоступных веб-приложениях не используются файлы «cookie» для хранения особо важной или критичной информации о клиентах (например, паролей), и что эти файлы имеют даты истечения срока действия (лучше раньше, чем позже). Рассмотрите возможность шифрования информации, хранящейся в используемых файлах «cookie».
- Рассмотрите возможность найма службы проверки на проникновение для оценки безопасности общедоступных веб-приложений не реже одного раза в год.

Индивидуальные рекомендации по защите финансовых данных для клиентов и сотрудников

Посоветуйте своим сотрудникам и клиентам следовать приведенным ниже рекомендациям по кибербезопасности в их личном поведении, чтобы повысить их готовность и защитить финансовые данные от киберугроз.

1. Обеспечьте внедрение основных практик в области кибергигиены на всех устройствах.

- Используйте надежные пароли на всех личных и профессиональных устройствах и рассмотрите возможность использования диспетчера паролей.
- Регулярно обновляйте операционные системы, другое ПО и приложения на своих компьютерах и мобильных устройствах.
- Установите антивирусное, антивредоносное ПО и защиту от программ-вымогателей для предотвращения, обнаружения и удаления вредоносных программ.
- Используйте брандмауэр для предотвращения несанкционированного доступа к компьютеру.
- Используйте продукты безопасности только от надежных компаний. Ознакомьтесь с отзывами о компьютерах и потребительскими изданиями, а также рассмотрите возможность консультации с производителем вашего компьютера или операционной системы.

2. Соблюдайте осторожность при работе с конфиденциальной информацией.

- Не отправляйте пароли от банковского счета или другие конфиденциальные данные финансового счета по незашифрованной электронной почте.
- Соблюдайте осторожность в отношении того, где и как вы подключаетесь к Интернету для связи с банком или другого обмена конфиденциальной личной информацией. Общедоступные сети Wi-Fi и компьютеры в таких местах, как библиотеки или бизнес-центры отеля, могут представлять опасность.

3. Противодействуйте фишингу.

- Не открывайте вложения из электронных писем сразу после получения и не переходите по ссылкам в незапрошенных или подозрительных электронных письмах. Остановитесь. Подумайте. Нажмите на кнопку.
- С подозрением относитесь к ситуациям, когда кто-то неожиданно обращается к вам через Интернет или по телефону и запрашивает личную информацию. Даже при общении с известными адресами сведите к минимуму обмен личной информацией по электронной почте.

ОБУЧЕНИЕ СОТРУДНИКОВ

- Обучайте своих сотрудников подотчетности и стратегиям минимизации человеческих ошибок, которые могут привести к раскрытию данных клиентов. Порекомендуйте им:
  - свести к минимуму доступ к данным клиентов и их передачу, получая его только для выполнения своих должностных обязанностей;
  - придерживаться строгих методов обеспечения безопасности на всех устройствах и учетных записях, которые работают с данными клиентов, посредством использования надежных паролей, двухфакторной аутентификации, обновления ПО, и воздерживаться от перехода по подозрительным ссылкам;
  - сообщать о любых потенциальных внутренних или внешних инцидентах в сфере безопасности, угрозах или неправильном обращении с данными техническим специалистам организации и/или высшему руководству.
- Убедитесь, что ваши сотрудники понимают эти требования и подписали документы, обеспечивающие соблюдение политик защиты данных и безопасности организации. Следите, чтобы они не нарушали эти политики и не взаимодействовали с клиентами в незащищенной среде.

УВЕДОМЛЕНИЕ КЛИЕНТОВ

- Обеспечьте понимание нормативных требований организации в отношении нарушений безопасности данных клиентов, чтобы гарантировать готовность к их соблюдению в случае подобных инцидентов.
- Когда ваша организация узнает о несанкционированном доступе к конфиденциальной информации клиентов, необходимо срочно провести расследование и определить вероятность того, что информация была или будет незаконно использоваться. Используйте передовые способы уведомления и незамедлительно сообщите пострадавшим клиентам следующие данные:
  - Общее описание происшествия и информацию, к которой был получен несанкционированный доступ.
  - Номер телефона для получения дополнительной информации и помощи.
  - Напоминание «сохранять бдительность» в течение следующих 24–12 месяцев.
  - Рекомендация о необходимости незамедлительного информирования о подозрениях в краже персональных данных.
  - Общее описание мер, предпринятых финансовым учреждением для защиты информации от дальнейшего несанкционированного доступа или использования.
  - Контактная информация бюро кредитных историй.
  - Любая другая информация, которая требуется в соответствии с соблюдаемыми организацией нормативными требованиями.

- Помните, что ни одно финансовое учреждение не будет отправлять электронные письма или звонить и запрашивать конфиденциальную информацию, которая у них уже имеется.
- Предполагайте, что запрос на получение информации из банка, где вы никогда не открывали счет, является мошенничеством.
- Перед предоставлением личной информации проверяйте достоверность подозрительного электронного письма или всплывающего окна. Обратите особое внимание на адрес электронной почты.

ИНСТРУКЦИИ ДЛЯ ДИРЕКТОРА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАЩИТА ОТНОШЕНИЙ С ТРЕТЬИМИ ЛИЦАМИ

ВЫЯВЛЕНИЕ РИСКОВ ЧЕРЕЗ ТРЕТЬИХ ЛИЦ

- Создайте и сохраните обновленный список всех отношений с поставщиками, а также всех предоставленных в них активов и данных.
- Проверьте данные, к которым у каждого поставщика или третьей стороны имеется доступ. Убедитесь, что этот уровень доступа соответствует принципу «минимальных привилегий».
- Оцените уровень риска отношений с поставщиками и сторонними организациями (низкий, средний, высокий), исходя из последствий получения несанкционированного доступа к их системам, для вашей организации.
- Начиная с поставщиков с высоким уровнем риска, оцените возможности систем кибербезопасности каждого поставщика. Хорошей отправной точкой является соблюдение соответствующих стандартов. Разработайте план регулярной оценки безопасности. Возможно, вы запланируете периодические выездные оценки поставщиков с наивысшим уровнем риска и/или более открытым доступом к данным клиентов.

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ ТРЕТЬИХ СТОРОН

- Проведите тщательную комплексную проверку. Разработайте требования к системам кибербезопасности в запросах вашей организации на предложения, контракты, непрерывность бизнеса, реагирование на инциденты и соглашения об уровне обслуживания с поставщиками. Согласуйте обязанности и обязательства в случае кибератак.
    - Узнайте о методах обеспечения кибербезопасности других третьих сторон, таких как финансовые организации, с которыми вы осуществляете операции или обмениваетесь данными. Кроме того, ваши поставщики и любые другие организации, с которыми вы обмениваетесь данными, должны соблюдать все требования к обеспечению кибербезопасности, которые соблюдает ваша организация.
- Используйте установленные и согласованные меры для осуществления контроля соблюдения стандартов кибербезопасности вашими поставщиками.
- Проверьте, предлагают ли ваши поставщики, обрабатывающие конфиденциальные данные, двухфакторную аутентификацию, шифрование и другие меры безопасности для всех используемых ими учетных записей.
- Убедитесь, что все устанавливаемое вами программное и аппаратное обеспечение оснащено системами безопасности для защиты процессов загрузки с помощью кодов аутентификации и отклонения загрузки в тех случаях, когда коды не распознаются.
- Если вы столкнулись с продукцией поставщика, которая является поддельной или не соответствует спецификациям, организуйте работу по решению вопроса или, если это невозможно, разработайте стратегию выхода.
- Проводите ежегодную оценку контрактов с поставщиками и убедитесь, что они продолжают соответствовать вашим стратегическим указаниям и требованиям в отношении безопасности данных. Включите в контракт положения о возврате ваших активов или данных после прекращения его действия, убедитесь, что активы или данные полностью удалены на стороне поставщика, и больше не предоставляйте ему доступ к вашим системам или серверам.

Рекомендации по выбору поставщиков с учетом обеспечения кибербезопасности

Задайте потенциальным поставщикам следующие вопросы, чтобы оценить их готовность и осведомленность в сфере кибербезопасности и, следовательно, влияние на профиль риска вашей организации:

1. **Какой опыт у них имеется?** Узнайте об истории поставщика в сфере обслуживания клиентов. Обслуживали ли они ранее клиентов, схожих с вашей организацией?
2. **Документировали ли они их соответствие установленным стандартам кибербезопасности,** например, модели Национального института по стандартизации и технологии (NIST) или стандарту ISO 27001, а также могут ли они предоставить отчет SOC2?
3. **Какие из ваших данных и/или активов им необходимы для предоставления своих услуг?** Запрашивают ли они какой-либо явно нецелесообразный доступ?
4. **Как они планируют обеспечить защиту активов и данных вашей организации, находящихся в их распоряжении?**
5. **Как они управляют собственными киберрисками?** Могут ли они предоставить информацию о своей цепочке поставок?
6. **Каков план аварийного восстановления и непрерывности бизнеса** в случае инцидента, касающегося активов и/или данных вашей организации?
7. **Как они будут информировать вашу организацию?** Каков их план передачи данных о тенденциях, угрозах и изменениях в своей организации?

ОБМЕН ИНФОРМАЦИЕЙ

- Убедитесь, что у вас есть четкие каналы связи и контакты для обмена сведениями о проблемах безопасности с поставщиками и партнерами вашей организации.
- Своевременно предоставляйте достоверную и действенную информацию о кибербезопасности внутренним и внешним заинтересованным сторонам (включая организации и государственные органы внутри и за пределами финансового сектора).
- Отслеживайте актуальные новости об опыте других организаций в работе с третьими сторонами в отношении угроз, уязвимостей, инцидентов и реакций, чтобы улучшить защиту своей организации, повысить ситуационную осведомленность и расширить возможности обучения. Членство в предоставляющих обмен информацией организациях, например, FS-ISAC, также способствует получению самых новых данных.

РУКОВОДСТВО ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ

ПОДГОТОВКА

- Совместно с высшим руководством вашей организации и другими соответствующими сотрудниками разработайте план реагирования на инциденты и план обеспечения непрерывности бизнеса, исходя из наиболее актуальных рисков, выявленных в ходе оценки киберрисков организации.
    - Разработайте сценарии угроз для инцидентов, связанных с наиболее приоритетными киберрисками организации. Сосредоточьтесь на наращивании потенциала для реагирования на эти сценарии.
    - Определите, составьте и представьте в вашей организации список контактных лиц для реагирования на инциденты.
    - Найдите и запишите контактные данные соответствующих местных и федеральных правоохранительных органов и должностных лиц.
    - Установите положения, определяющие, о каких типах инцидентов необходимо сообщать, когда и кому.
    - Определите и представьте в письменном виде указания, определяющие, как быстро персонал должен реагировать на инциденты и какие действия должны быть выполнены на основе соответствующих факторов, таких как функциональное и информационное воздействие инцидента, а также вероятной возможности восстановления после него.
    - Сообщите всем сотрудникам, чтобы в случае инцидента они связывались с вашей технической командой. Обычно это ИТ-персонал и/или директор по информационной безопасности / директор по ИТ / другой подобный менеджер.
    - Выполните развертывание решений для мониторинга действий сотрудников и выявления угроз и инцидентов.
    - Включите планы по обеспечению непрерывности бизнеса для координации работы организации с поставщиками и основными клиентами во время чрезвычайной ситуации, в том числе при необходимости осуществления руководства или проведения альтернативных бизнес-операций.
    - Включите определенные в письменном виде процедуры отключения и перезапуска системы в чрезвычайной ситуации.
    - Обеспечьте разработку и тестирование методов извлечения и восстановления резервных данных. Периодически проверяйте резервные данные на предмет их целостности.
    - Заключите соглашения и процедуры ведения коммерческой деятельности в альтернативном учреждении/центре.
    - Обеспечьте работу четкого канала распространения для всех клиентов.

ОБУЧЕНИЕ

- Организуйте небольшие теоретические занятия со всеми сотрудниками или представителями персонала всех уровней, в том числе с руководителями организации, специалистами по связям с общественностью, сотрудниками юридического отдела и отдела нормативно-правового соответствия.
- Определите или лучше примите участие в отраслевых теоретических занятиях, связанных с деятельностью вашей организации.
- Разработайте процедуру проверки того, что сделанные в ходе занятий выводы включены в стратегию обеспечения кибербезопасности компании.

РЕАГИРОВАНИЕ

- Внедрите действия плана реагирования на инциденты, чтобы свести к минимуму последствия, в том числе в отношении подрыва репутации.
- Определите поврежденные или находящиеся под угрозой системы и оцените повреждения.
- Для уменьшения ущерба выполните удаление (отключение) поврежденных активов.
- Начните запись всей информации сразу же после того, как команда выразит подозрения по поводу возможного инцидента. Попытайтесь сохранить доказательства инцидента при отключении/разделении поврежденного идентифицируемого актива, например, соберите данные о конфигурации системы, сети и журналов обнаружения вторжений из поврежденных активов.
- Уведомите соответствующие внутренние стороны, сторонних поставщиков и органы власти и при необходимости запросите поддержку.
- Инициируйте меры по уведомлению клиентов и оказанию помощи в соответствии с законами, нормативно-правовыми актами и межведомственным руководством.
- Используйте такие платформы обмена угрозами, как FS-ISAC или MISP для уведомления об угрозах других организаций из вашей отрасли.
- Задокументируйте все предпринятые во время инцидента шаги для последующего анализа.

ВОССТАНОВЛЕНИЕ

- По возможности восстановите активы с использованием периодических «точек восстановления» и используйте резервные данные для восстановления систем до последнего известного «исправного» состояния.
- Обеспечьте создание обновленных «чистых» резервных копий из восстановленных активов и убедитесь, что все резервные копии критически важных активов хранятся в физически защищенном месте.
- Выполните тестирование и убедитесь, что инфицированные системы полностью восстановлены. Убедитесь, что затронутые системы нормально функционируют.

АНАЛИЗ

- Обсудите «сделанные выводы» после инцидента. Организуйте встречу с руководящим составом, доверенными советниками и поставщиками услуг поддержки аппаратного обеспечения для проведения анализа возможных уязвимостей или выработки рекомендаций по внедрению новых мер.
- По возможности определите уязвимости (будь то программное обеспечение, оборудование, бизнес-операции или поведение персонала), которые привели к инциденту и разработайте план по их устранению.
- Разработайте план мониторинга для выявления аналогичных или потенциально возможных инцидентов, связанных с выявленными проблемами.
- Поделитесь сделанными выводами и информацией об инциденте на платформах обмена угрозами, таких как FS-ISAC.
- Включите сделанные выводы в протоколы реагирования на произошедшие в организации инциденты.

ПРОГРАММЫ-ВЫМОГАТЕЛИ: ПРЕДОТВРАЩЕНИЕ И ЗАЩИТА

ЗАЩИТА В РЕАЛЬНОМ ВРЕМЕНИ

Программы-вымогатели представляют все большую и большую угрозу, с тех пор как злоумышленники нашли способ монетизации вредоносных программ, парализуя работу компьютерных систем и требуя выкуп за восстановление исходного состояния. В отличие от других вредоносных программ, которым для эффективной работы часто приходится оставаться скрытыми в течение длительного времени, программы-вымогатели действуют быстро через адресный фишинг, скомпрометированные веб-сайты и поврежденные загрузки. Финансовые учреждения считаются выгодными целями и особенно уязвимы перед атаками программ-вымогателей, которые угрожают быстрому и эффективному перемещению денежных средств. Однако далеко не всегда злоумышленники сдерживают свое обещание: даже после выплаты выкупа они могут не удалить вредоносную программу и не вернуть конфиденциальную информацию.

- Инвестируйте в системы защиты от вредоносных программ, которые адаптируются к угрозам в реальном времени с помощью анализа данных.
- Оцените безопасность всех подключенных к сети устройств, на которых хранится конфиденциальная или важная информация. Подключайте все вспомогательные системы к отдельной сети.
    - Будьте осторожны при развертывании Интернета вещей и использовании смарт-устройств в рабочей среде, поскольку их системы безопасности зачастую более уязвимы, либо у них может вообще не быть систем безопасности. Кроме того, такие устройства могут использоваться как точки доступа к важным системам.
    - Подумайте о безопасности настроек при удаленной работе. Убедитесь, что инструменты безопасности работают при отсутствии сети для отслеживания всего веб-трафика.
- Стимулируйте обучение сотрудников в области фишинговых атак и необходимости защиты надежным паролем.
- Рассмотрите возможность внедрения многофакторной аутентификации в вашей организации.
- Регулярно обновляйте все системы и программное обеспечение. По возможности измените настройки и разрешите автоматическое обновление.
- Разработайте план действия в кризисных ситуациях и реагирования на инциденты для борьбы с атаками программ-вымогателей и потерей ценных данных.
- Подготовьте план внешней связи на случай атаки программ-вымогателей.

РЕЗЕРВНОЕ КОПИРОВАНИЕ ДАННЫХ

- Инвестируйте в безопасные, регулярно обновляемые системы резервного копирования, обеспечивающие защиту ваших данных.
    - При использовании USB-накопителей или жестких дисков физически отключайте эти устройства от компьютеров, подключенных к сети, после завершения резервного копирования.
    - При использовании облачного хранилища оборудуйте сервер шифрованием высокого уровня и многофакторной аутентификацией.
- Создайте копию главной книги, предназначенную только для чтения, на случай аварийного восстановления в худших условиях.
- Разрабатывайте системы, которые выполняют автоматическое восстановление и исправление данных.
- Разработайте сценарии для оценки времени восстановления критических данных и бизнес-служб.

Оценка готовности вашей организации к атакам программ-вымогателей

При разработке плана предотвращения атак программ вымогателей и защиты от них рассмотрите следующие вопросы.

1. **Регулярно** ли в вашей организации выполняется **плановое резервное копирование**?
    - Отключены ли эти резервные копии от сети (с помощью облачного хранилища или физического отключения USB-накопителей / жестких дисков?
2. Подключены ли к сети вашей организации какие-либо **вспомогательные устройства**?
    - Могут ли они быть переподключены к другим сетям, в которых не хранится конфиденциальная информация?
3. Осознают ли в вашей организации **нормативные и правовые риски,** связанные с выплатой выкупа?
    - В каждой стране действуют свои правовые руководства, которые часто обновляются.
4. Регулярно ли в вашей организации обновляется программное обеспечение и системы? Обновления **автоматизированы**?
5. Есть ли в вашей организации **план борьбы с атаками программ-вымогателей** и предотвращения потери ценных данных?
6. Есть ли у вашей организации **полис киберстрахования**? Если есть, что покрывает план страхования при атаках программ-вымогателей?
    - Некоторые планы прямо запрещают выплату выкупа, в то время как другие покрывают такие выплаты в рамках полиса.

НОРМАТИВНО-ПРАВОВАЯ СРЕДА

- Оцените соответствующие нормативные и правовые руководства по программам-вымогателям для вашей операционной среды.
  - Изучите рекомендации для конкретной страны. Разработайте план по периодической оценке изменений в руководствах.
  - Изучите рекомендации для конкретного финансового сектора.
  - Изучите международные правовые и нормативные требования.
- Оцените риски, связанные с выплатой выкупа. В некоторых случаях выплата выкупа может нарушить действующие санкции в отношении злоумышленников.
- Поддерживайте контакт с правоохранительными органами. Организуйте способы коммуникации для быстрого обмена информацией в случае атаки.
- Оцените преимущества и недостатки полисов киберстрахования от атак программ-вымогателей.

ПОДГОТОВКА СПЕЦИАЛИСТОВ

ОПРЕДЕЛЕНИЕ ПОТРЕБНОСТЕЙ

- Определите ваши требования по нагрузке.
  - Оцените сложность выполняемых операций и скорость, с которой они должны выполняться.
  - Оцените необходимость увеличения количества сотрудников в экстренном случае и внедрения более продвинутых технологий для снижения вариантов атаки.
- Определите требования, предъявляемые к сотрудникам.
  - Оцените компетентность, гибкость и скорость мышления специалистов по кибербезопасности в вашей организации.
  - Определите идеальную иерархию штатных должностей и сферы, в которых предпочтение должно отдаваться многофункциональности.
- Определите требуемые знания, навыки, способности и области компетентности для специалистов на основе тех рабочих функций, которые они должны выполнять в организации.
- Определите слабые стороны специалистов по кибербезопасности, уже работающих в вашей организации.
  - Используйте существующие инструменты, такие как модель NICE, для проведения внутренней оценки ролей и обязанностей.

ДОПОЛНИТЕЛЬНОЕ ВНУТРЕННЕЕ ОБУЧЕНИЕ И КАРЬЕРНЫЙ РОСТ

- Составьте планы карьерного роста и обозначьте возможные пути развития для специалистов по кибербезопасности.
- Определите направления переобучения и переориентирования сотрудников на должности по кибербезопасности в вашей организации.
  - Продумайте альтернативные способы привлечения сотрудников в сферу кибербезопасности, исходя из их интересов и возможностей.
  - Расширяйте программы повышения квалификации и переобучения, а также стимулируйте переводы на другие должности внутри вашей организации.
- Поощряйте обучение и повышение квалификации как внутри вашей организации, так и в других учебных центрах.
  - Предоставьте возможности для дальнейшего обучения и профессиональной аттестации.
- Отслеживайте данные по оттоку и притоку кадров.
  - Регулярно оценивайте данные по оттоку и притоку кадров, чтобы определить, отвечают ли программы обучения и карьерного роста требованиям сотрудников.

УЛУЧШЕНИЕ НАБОРА НОВЫХ СОТРУДНИКОВ

- Улучшайте объявления о вакансиях, четко указывая должностные обязанности, согласованные внутри вашей организации.
  - Используйте существующие инструменты, такие как модель NICE, чтобы выделить релевантные наборы навыков.
- Собирайте данные о найме в процессе приема заявлений, фиксируя типы кандидатов и предыдущий опыт работы.
  - Систематизируйте сбор данных и обменивайтесь ими в компании для согласованного подбора и улучшения поиска кадров.
  - Периодически оценивайте данные по найму для выявления недочетов в охвате.
- При оценке потенциала кандидата исходите из нескольких показателей.
  - Рассмотрите возможность систематизированной оценки при найме.
  - Принимайте во внимание наличие дипломов, сертификатов и опыта работы в конкретной сфере.
  - Принимайте решение о найме на основании нескольких показателей, а не одного (как, например, инженер высшей категории).

Основные подходы

Применяйте следующие стратегические подходы к подготовке специалистов по кибербезопасности.

1. **Расширьте способы подбора** новых кадров.
   - Поддерживаете ли вы отношения с университетами и техническими колледжами?
   - Предлагаете ли вы стажировку и обучение в области кибербезопасности?
2. **Соотнесите имеющиеся способы подбора кадров** с открытыми вакансиями.
   - Эффективно ли ваш отдел кадров представляет требуемые навыки в публикуемых должностных обязанностях?
3. **Организуйте переобучение сотрудников** в специалистов по кибербезопасности.
   - Могут ли сотрудники переобучиться на специалистов по кибербезопасности в вашей организации?
4. **Уменьшайте потребности** в специалистах по кибербезопасности посредством **технологических инноваций.**
   - Есть ли у вас соглашения со сторонними поставщиками услуг о предоставлении резервных ресурсов в случае экстренной необходимости?
5. **Стимулируйте** ваших сотрудников.
   - Инвестирует ли ваша организация в талантливых специалистов?
   - Предоставляет ли ваша организация возможности для карьерного роста в области кибербезопасности?