RIIGI INFOSÜSTEEMI AMET

Краткое руководство по кибербезопасности для организаций

2019

Краткое руководство составлено акционерным обществом BCS Koolitus, по заказу Департамента государственной инфосистемы (RIA), в рамках программы «Повышение осведомленности информационного общества» при финансовой поддержке Европейского фонда регионального развития.

Содержание

Приветственное слово

Сильные компании строят более сильное общество

В 2018 году в Эстонии вступил в силу Закон о кибербезопасности, установивший требования к кибербезопасности для компаний и учреждений, чья деятельность жизненно необходима - государственных организаций, портов, энергетических компаний, операторов связи и других. Принятие закона показало общее понимание того, что для определенных организаций кибербезопасность необходима. Для некоторых организаций это требование установлено законодательно.

В то же время кибербезопасность эстонского народа напрямую зависит от того, насколько надежно все другие малые компании и учреждения, для которых аналогичные требования не установлены законодательно, могут защитить себя и своих клиентов (их данные). Сумма, которую предприятия теряют в результате финансового мошенничества из-за взлома учетных записей электронной почты, увеличивается с каждым годом. Преступники постоянно находят новые уязвимости в информационных системах и используют их для кражи личных данных клиентов.

Все это заставляет задуматься о том, как небольшая или средняя компания может защитить себя от подобных современных атак. Оплата руководителей или групп по информационной безопасности может выходить за пределы возможностей компаний, стандарты кибербезопасности могут показаться столь громоздкими и ресурсоемкими, что их внедрение не представляется коммерчески обоснованным. Что же тогда делать?

Кибербезопасность не должна сводиться к тому, чтобы делать все или же ничего. Начинать надо с небольших шагов и постепенно продвигаться вперед - так же, как компании постоянно пересматривают и улучшают свою деятельность и организацию работы.

Данное краткое руководство по кибербезопасности предназначено для того, чтобы помочь организациям сделать первые шаги для повышения кибербезопасности в рамках своей деятельности. Здесь можно найти основные принципы - как защитить своих клиентов, системы, сотрудников и торговую марку. Необходимость этих принципов должна быть понятна каждому руководителю, и любой поставщик IT услуг, осведомленный об информационной безопасности, должен иметь возможность применять эти меры.

Уровень безопасности всегда возможно повысить технически. Однако начинать следует с того, что кибербезопасность - это не только задача IT отдела, но также и других руководителей. Чем яснее руководитель понимает необходимость реализации этих мер, тем лучше он сможет управлять своей командой и ресурсами. Департамент государственной инфосистемы (RIA) готов стать вашим лучшим советником в этом направлении.

Маргус Ноормаа
Генеральный директор Департамента государственной инфосистемы (RIA)

1 Знайте, какое аппаратное и программное обеспечение вы используете

Чтобы успешно защищать сеть своей организации, сначала необходимо получить обзор устройств и программного обеспечения в этой сети. Поэтому инвентаризация - это первый и очень важный шаг в создании защищенной системы. Если нет информации о том, какие устройства или программное обеспечение должно быть в сети, тогда невозможно обнаружить неизвестные или неавторизованные устройства и программное обеспечение. Именно такие устройства или программное обеспечение могут быть использованы злоумышленниками для получения доступа к офисной сети. Если неизвестно, какое программное обеспечение используется, то невозможно провести его обновление. Существует также риск того, что может быть установлено программное обеспечение, которое может заразить систему вредоносным программным обеспечением (например, нелегальным программным обеспечением для загрузки музыки / фильмов). Для каждого устройства в офисной сети необходимо знать следующую информацию:

1) название устройства;
2) IP-адрес;
3) назначение устройства или причина его нахождения в сети (чей-то компьютер, сервер, сетевое устройство и т. д.);
4) список программного обеспечения, установленного на вашем устройстве.

1.1 Проведите инвентаризацию вашего оборудования

Во-первых, нужно определить, какие устройства находятся в сети. Даже если это небольшая сеть с несколькими устройствами, эта информация должна быть задокументирована. Если это не будет сделано, то устройства могут остаться незащищенными. Злоумышленники ищут незащищенные устройства для атаки на корпоративную сеть. Обзор устройств в сети также необходим, когда происходит смена IT специалистов, потому что им нужна информация о сети и устройствах в ней.

Если ваша корпоративная сеть больше, чем несколько компьютеров, рекомендуется использовать программное обеспечение, которое автоматически выполняет инвентаризацию. Ручная инвентаризация может привести к ошибкам, и, если в наличии больше оборудования, это займет много времени. Регистр аппаратного обеспечения должен также включать любые устройства, которые в данный момент отсутствуют в сети, но могут подключиться к ней или, в случае кражи которых, могут быть потеряны данные.

1.2 Проведите инвентаризацию вашего программного обеспечения

После того, как вы получите обзор устройств в сети, необходимо определить, какое программное обеспечение в них используется. Это делается для того, чтобы убедиться, что программное обеспечение обновлено и на устройствах установлено нужное программное обеспечение. Для инвентаризации программного обеспечения также целесообразно использовать программы, которые способны автоматически собирать данные. Автоматическая инвентаризация программного обеспечения помогает, среди прочего, определять, когда на устройство было добавлено новое программное обеспечение. Собранные данные о программном обеспечении должны быть связаны с регистром аппаратного обеспечения, чтобы все устройства и связанное с ними программное обеспечение можно было отслеживать в одном месте.

Спросите у IT специалиста!

Для инвентаризации аппаратного и программного обеспечения доступны как бесплатные, так и платные программы. Платное программное обеспечение обычно предлагает больше функциональности. Узнайте у IT специалистов вашей организации или поставщика услуг о соответствующем программном обеспечении.

1.3 Рассмотрите возможность централизованного управления устройствами

Чтобы лучше управлять своим оборудованием и программным обеспечением, следует рассмотреть возможность использования централизованного решения. Оно позволяет централизованно управлять вашими устройствами и определять, какое программное обеспечение должно быть на них установлено, устраняя при этом необходимость установки дополнительного программного обеспечения для инвентаризации. Централизованное управление позволяет как проводить инвентаризацию, так и составлять требования к безопасности оборудования. Некоторые программы централизованного управления могут удалять данные с устройств через Интернет, что полезно, если сотрудник потерял устройство или его украли.

Спросите у IT специалиста!

Существует несколько решений для централизованного управления, в зависимости от того, какие устройства (компьютеры, интеллектуальные устройства) используются. Обычно они являются платными. Узнайте у своих IT специалистов или поставщика услуг подходящие для вашей компании решения.

1.4 Создайте правила использования личных устройств в рабочей среде

В наши дни сотрудники все чаще хотят использовать для работы личные персональные устройства. Наиболее распространенными являются смарт устройства (телефоны и планшеты), также все чаще используются персональные компьютеры. Кроме того, часто на работу приносят собственные USB-накопители и внешние жесткие диски, которые позволяют быстро и легко передавать данные из внутренней сети на внешние носители. Если сотрудникам разрешено использовать персональное оборудование, то для этого должны быть установлены правила, поскольку сотрудники работают с данными компании на личных устройствах. По возможности, правила должны разрабатываться в сотрудничестве с IT персоналом.

При разработке правил использования личных устройств следует:

1) определить, какие требования безопасности предъявляются к персональным устройствам. Например, обязательно надо требовать, чтобы устройства были защищены паролем, и на них было бы установлено антивирусное программное обеспечение. Если на устройстве хранятся конфиденциальные данные, то оно должно быть зашифровано;
2) составить список устройств и операционных систем, которые нельзя использовать в организации, таких как устройства с уязвимостями или устройства, которые

больше не поддерживаются производителем программного обеспечения (например, компьютеры под управлением Windows XP должны быть запрещены). Кроме того, должно быть запрещено использование персональных сетевых устройств (персональные роутеры, свитчи, Wi-Fi устройства и т. д.), которые могут создавать помехи в корпоративной сети;

3) по возможности вести список оборудования, которое работники хотят использовать. Он должен включать имя сотрудника, название устройства, список программного обеспечения и т. д.
4) при необходимости установить правило, запрещающее хранение связанной с работой информации на личных устройствах.

Работники должны ознакомиться с правилами и нормами и дать своё согласие, подписав соответствующий документ (в противном случае им будет запрещено пользоваться личным устройством на работе).

2 Защищайте свою собственность

Как только будет получено представление о том, какое оборудование и программное обеспечение используется в сети офиса и у сотрудников, то необходимо начать защищать их.

Поскольку оборудование и различные услуги (веб-сайт, программное обеспечение для бизнеса и т. д.) могут предоставляться поставщиком услуг или уже могут иметь некоторую форму защиты программного обеспечения (брандмауэр, антивирус), может показаться, что оборудование и программное обеспечение, используемое на предприятии, уже защищены. На самом деле этого недостаточно для защиты от угроз. Для обеспечения более надёжной защиты данных и оборудования необходимо принять дополнительные меры.

2.1 Предоставляйте права доступа разумно

Атаки и вирусы обычно распространяются через пользователей. Чем больше прав у пользователя, тем легче будет действовать злоумышленнику или вирусу.

Поэтому при каждом предоставлении доступа нужно подумать о том, нужны ли эти разрешения (например, доступ к общей папке или программному обеспечению, права администратора на компьютере) для работы. Если решается, что доступ действительно необходим, то он должен предоставляться на основе принципа наименьшего права, то есть работнику должно быть предоставлено столько прав, сколько ему нужно для работы, и не более. Часто идут лёгким путём и предоставляют доступ ко всему каталогу, который может позволить сотруднику получить доступ к данным, к которым у него не должно быть доступа. Даже если сотрудник ничего не делает с этим доступом, им могут воспользоваться злоумышленники.

> **Совет!**
>
> Делитесь правами доступа через группы. Это облегчает обмен правами и дает хороший обзор. Также, когда сотрудник уходит, его легко удалить из соответствующих групп вместо того, чтобы просматривать каталоги один за другим и искать, к чему у него был доступ.

Сотрудникам обычно не требуются права администратора на рабочем компьютере.

Наличие прав администратора имеет ряд рисков:

- Сотрудник может устанавливать на свои компьютеры программы, которые могут привести к уязвимостям в системе безопасности и установке вредоносных программ.
- Ущерб, нанесенный вредоносным программным обеспечением будет больше, если у сотрудника есть права администратора.
- Злоумышленникам будет проще взять компьютер под контроль и т. д.

Если требуются права администратора, то для компьютера должна быть настроена отдельная учетная запись локального пользователя, которая будет использоваться только при необходимости, а не для повседневных операций. Это снижает вероятность того, что пользователь случайно установит вредоносное программное обеспесение,

и, если произойдёт утечка информации из учетной записи сотрудника, злоумышленник не сразу получит права администратора. Если это персональный компьютер сотрудника, то надо следовать пункту 1.4 «Создайте правила использования личных устройств в рабочей среде», но в этом случае также следует рекомендовать отдельную учетную запись для рабочей информации.

Спросите у IT специалиста!

Обратитесь к своему IT специалисту или поставщику услуг с просьбой о регулярном обзоре используемых учетных записей администратора.

Если IT специалист или поставщик услуг предоставляет права доступа, то они также должны задокументировать эти разрешения (когда, для чего, кому), чтобы иметь актуальный обзор того, кто имеет доступ. Эта информация также полезна, когда сотрудник уходит, поскольку тогда известно, какие права должны быть закрыты.

Если произойдет связанный с безопасностью инцидент, то такая документация может предоставить информацию о том, что произошло.

2.2 Регулярно обновляйте программное обеспечение

Современное рабочее место предполагает использование разного рода программного обеспечения. В программном обеспечении постоянно обнаруживаются уязвимые места, которые могут быть использованы злоумышленниками для установки вредоносных программ, получения контроля над компьютером и / или кражи данных. Поэтому регулярные обновления программного обеспечения очень важны и являются одним из самых простых способов защиты данных организации.

Если возможно автоматическое обновление программного обеспечения (например, для компьютеров, смарт устройств), то его следует включить. Однако если программное обеспечение не имеет такой функции (например, некоторые специальные программы или программное обеспечение сетевых устройств), это необходимо сделать вручную (самостоятельно, с помощью IT специалистов или поставщика услуг) или с помощью решения, которое производит обновления автоматически. Например, многие из современных антивирусных решений включают функцию автоматического обновления программ.

Если версия программного обеспечения или аппаратного обеспечения больше не поддерживается или не обновляется производителем, то следует установить новую версию. Например, Microsoft с 2020 года не будет поддерживать компьютеры с операционной системой Windows 7, но они все еще используются во многих организациях. В этом случае определенно следовало бы перейти на последнюю версию операционной системы Windows, потому что даже если уязвимости в старом программном обеспечении еще не обнаружены, их обнаружение является лишь вопросом времени. Стоит исходить из принципа, что если в безопасности имеется уязвимость, то имеется и злоумышленник, который с радостью воспользуется ею.

2.3 Организуйте защиту компьютерной сети вашей компании и ее пользователей

Граница между общедоступным Интернетом и офисной сетью называется периметром. Чем меньше подозрительного трафика попадает в офисную сеть, тем меньше риск для сотрудников и оборудования, использующего офисную сеть. Защита периметра - это брандмауэр, который выступает в роли посредника или шлюза между общедоступной и офисной сетью и отфильтровывает опасный трафик. Межсетевые экраны с большим количеством функций могут обнаруживать и предотвращать атаки в офисной сети. Такие брандмауэры могут дополнительно ограничивать или разрешить сотрудникам доступ к определённым страницам. Например, можно заблокировать известные опасные страницы или же другие страницы сомнительного назначения, которые могут привести к заражению вирусами. Также можно контролировать, какие приложения сотрудники используют для доступа в Интернет (например, можно запретить загрузку фильмов и музыки из Интернета).

Поскольку многие вирусы и атаки проходят через электронную почту, необходимо иметь защиту от спама. Такое программное обеспечение удаляет подозрительные сообщения (спам, фишинг, вирусы и т. д.), чтобы они не доходили до сотрудников. Большинство почтовых серверов содержат некоторую форму защиты от спама, но их функциональные возможности часто ограничены. Защита от спама также существует, например, как внешняя служба в облаке или на хостинге (расположенная вне офисной сети) или как отдельный сервер в офисной сети. Более качественное антиспамовое программное обеспечение имеет ряд функций, которые облегчают жизнь сотрудникам - заказ отчета о спаме, блокировка отправителей и многое другое.

Из-за изобретательности злоумышленников вредоносные программы все еще время от времени попадают к пользователям. Поэтому важно, чтобы на всех устройствах было установлено антивирусное программное обеспечение, защищающее их от вредоносных программ. Кроме того, надо следить за тем, чтобы была установлена последняя версия антивирусного программного обеспечения и она постоянно обновлялась, а также, что все функции включены, потому что только в этом случае защита будет эффективной.

2.4 Блокируйте доступ к данным на потерянных и украденных устройствах

Неизбежно, что иногда сотрудники теряют свое оборудование (смартфоны, планшеты или ноутбуки и т. д.) или оно может быть украдено. Поскольку устройства могут содержать конфиденциальную деловую информацию или другую информацию, которая не должна находиться в руках третьих лиц, следует спланировать, что делать в такой ситуации.

Одним из хороших решений является централизованное управление, описанное в главе 1.3 «Рассмотрите возможность централизованного управления устройствами», которое позволяет удаленно блокировать, определять местоположение или удалять устройство в случае его утери. В смартфоны и планшеты также установлены бесплатные приложения, которые позволяют настраивать централизованное управление, и их тоже стоит использовать.

Шифрование компьютера также помогает предотвратить доступ к данным. В этом случае данные присутствуют на компьютере, но злоумышленник ничего не может с ними сделать. Существуют различные варианты шифрования, доступно много программ, также можно использовать программу шифрования BitLocker, поставляемую с Windows 10.

2.5 Позаботьтесь о физической защите ваших данных и устройств

В дополнение к программным мерам защиты следует также обратить внимание на физическую защиту устройств. Все оборудование, содержащее важные данные, должно быть защищено от доступа посторонних лиц. Например, брандмауэр бесполезен, если незнакомец может свободно ходить по офису, попасть в помещение, где находится сервер и, таким образом, иметь прямой доступ к устройствам.

Серверы, сетевые устройства и другие важные устройства, содержащие данные, должны располагаться в отдельном шкафу для устройств или в выделенной серверной комнате. Дверь шкафа или серверной комнаты должна быть заперта, а ключ должен храниться в безопасном месте. Также нужно вести журнал посещений серверной комнаты (записывать, кто, когда и для каких целей посещал), чтобы была возможность определить, кто и когда там был.

Спросите у IT специалиста!

Если сервер размещен удалённо, надо убедиться, что у поставщика услуг есть информация о том, кто имеет физический доступ к серверу и кто его использовал.

Чтобы сервер работал бесперебойно, он должен быть достаточно охлажден (с кондиционером в серверной комнате) и подключен к UPS, чтобы защитить его от сбоя питания. В противном случае сервер может отключиться в жаркий летний день или данные могут быть повреждены в случае сбоя питания. Кондиционер также следует подключить к UPS, иначе в случае сбоя питания сервер может продолжать работать, но в конечном итоге отключиться из-за перегрева.

Если в офисе на стенах есть сетевые розетки, которые не используются, то они не должны иметь доступа к сети (это может настроить IT специалист или поставщик услуг). В противном случае может случиться так, что любой человек через сетевые розетки подключится к своему компьютеру и получит доступ ко всему офисному оборудованию. Следующим шагом будет настройка компьютеров и серверов, которые будут логически расположены в отдельных сетях, то есть, если кто-то получит доступ к компьютерной сети, он не получит немедленный доступ к серверам.

Не менее важно обучать сотрудников, чтобы они, покидая компьютер, не оставляли его разблокированным, и чтобы в общедоступных местах устройства не были забыты и не использовались посторонними лицами.

3 Защищайте своих сотрудников

Для защиты данных и пользователей важно, чтобы любой доступ к системам требовал пароль или другую форму аутентификации. Пароль должен быть достаточно сложным, чтобы его было трудно угадать. Если система не защищена паролем или используемый пароль легко подобрать, то вредоносные программы и злоумышленники будут иметь значительно больше шансов получить доступ к системе. Это может привести к утечке и потере данных или даже изменению важных данных.

3.1 Создайте защищённую политику использования паролей

Аутентификация - это действие, при котором система определяет, является ли человек, который обращается к системе тем, за кого он себя выдаёт. Обычно для идентификации используется пароль или сертификат.

Для обеспечения безопасности офисной сети необходимо установить правила создания пароля и правила регулярной смены пароля. В настоящее время рекомендуется менять пароль каждые шесть месяцев, и его длина должна быть не менее 15 символов. Также не рекомендуется требовать слишком длинный и сложный пароль, поскольку пользователи могут записать его где-нибудь на бумаге. Поэтому желательно использовать контрольную фразу вместо обычного пароля. Контрольная фраза состоит из четырех-пяти слов, составляющих предложение (например: 1Hobune.On.We.Aar3s) – оно длиннее, но проще для запоминания, чем пароль со случайными символами. В пароле желательно использовать маленькие и заглавные буквы, символы (точка, запятая, восклицательный знак и т. д.) между словами. Пароль должен легко запоминаться, но при этом не угадываться.

Если настройки системы позволяют, то все предложенные выше параметры должны устанавливаться автоматически, так как пользователь всегда выбирает самый простой путь для создания пароля. Если системная настройка невозможна, то пароли необходимо регулярно менять вручную и постоянно напоминать об этом пользователям. Небольшие компании обычно не имеют отдельной политики паролей, но важно, чтобы пароли использовались в соответствии с надлежащей практикой безопасности.

Спросите у IT специалиста!

Уточните у вашего IT специалиста или поставщика услуг, отвечает ли текущая политика паролей современным стандартам защиты.

3.2 Используйте многоэтапную аутентификацию

В результате растущей популярности облачных сервисов компании все чаще используют услуги, которые являются общедоступными. Когда услуга является общедоступной, ее легче атаковать. Если какие-либо из этих коммерческих служб (Office 365, Gmail, Dropbox и т. д.) позволяют включить многоэтапную аутентификацию, то этим надо воспользоваться. Это означает, что в дополнение к паролю требуется другой метод аутентификации, такой как ввод кода, проверка по телефону, использование ID карты и т. д. Когда реализована многоуровневая аутентификация, злоумышленники не могут

получить доступ к системе даже при утечке пароля, поскольку у них нет другого компонента, необходимого для аутентификации.

3.3 Упростите использование паролей

Поскольку большинство систем требуют использования паролей, у сотрудника может быть много разных аккаунтов и паролей. В этом случае пользователи начнут записывать их на бумаге, использовать один и тот же пароль в нескольких местах, если это возможно, или выбирать слишком простые пароли. Одним из решений, помогающих пользователям, является внедрение программного обеспечения для управления паролями, которое позволяет им безопасно управлять своими паролями. Для этого доступно различное программное обеспечение, в том числе и бесплатное.

Если в использовании много устройств, то можно использовать централизованное решение для управления пользователями. Например, в Microsoft Windows существует служба каталогов Active Directory (AD). Домен AD - это сервис, который обеспечивает интегрированную аутентификацию в среде Windows. Это позволяет пользователям входить на любое устройство в домене с одним и тем же именем пользователя и паролем. Например, если до введения домена у пользователей был отдельный пароль для компьютера, службы электронной почты и общей папки, то домен позволяет для всего использовать один пароль. Домен AD требует наличие сервера Windows. Существуют другие аналогичные решения, для которых не требуется сервер, например Azure AD, для которого требуются лицензии на программное обеспечение Office 365. Некоторые финансовые программы также могут быть связаны с доменом AD или Azure AD. Централизованное управление пользователями, среди прочего, облегчает закрытие доступа к информации и устройствам, когда пользователь уходит, потому что это может быть сделано из центральной точки управления.

4 Научитесь распознавать атаки

Система безопасна настолько, насколько безопасно ее самое слабое звено. Часто самым слабым звеном являются пользователи. Поэтому киберпреступники пытаются получить доступ к системе главным образом через пользователей, отправляя им сообщения, которые могут содержать вирусы или фишинговые электронные письма, пытаясь получить пароли, банковские реквизиты или деньги. В Интернете также есть сайты, которые пытаются украсть данные и деньги у пользователей или же содержат вирусы. Поэтому сотрудников нужно учить как распознавать атаки и бороться с ними. Информирование и обучение сотрудников также является одним из наиболее важных шагов в защите компании.

4.1 Повышайте осведомленность сотрудников

В последние годы киберпреступники значительно продвинулись в развитии, и становится все сложнее понять, является ли полученное письмо или веб-страница мошеннической или нет. Сотрудники должны быть осведомлены о наиболее распространенных типах атак, о том, как их распознать и как с ними бороться. Такая информация и рекомендации могут быть предоставлены IT специалистами компании или поставщиком услуг.

Наиболее распространенными типами атак являются фишинговые письма и веб-сайты, которые пытаются заставить пользователя ввести свои данные (*фишинг*). Фишинг - это наиболее доступный и самый простой способ для киберпреступника получить доступ к устройствам организации.

Типичные примеры мошеннических писем:

- Электронные письма, с прикрепленными счетами от деловых партнеров, которые просят быстро оплатить необходимую сумму на иной банковский счет, чем обычно.
- Электронное письмо от, казалось бы, главного исполнительного директора или члена совета директоров бухгалтеру компании с просьбой сделать перевод на банковский счет.
- Сообщение от некоторых поставщиков услуг (электронная почта, банковские услуги, интернет-провайдер и т. д.) с просьбой предоставить личные данные и пароль пользователя.

Полезно знать!

Важно помнить, что банк или поставщик услуг электронной почты не должны запрашивать ваши пароли!

Если какое-либо электронное письмо, которое вы получаете, кажется подозрительным, всегда надо обращаться к IT персоналу компании или поставщику услуг, чтобы они просмотрели это письмо. Даже если окажется, что письмо было безопасным, лучше лишний раз проверить, чем потом сожалеть.

Сотрудники должны быть обучены распознавать мошеннические и фишинговые электронные письма и опасные веб-сайты:

1. Нужно смотреть на адрес электронной почты отправителя - хотя он может казаться подлинным, в самом написании адреса могут быть небольшие изменения.

Например, вместо “@eesti.ee” может быть “„@eetsi.ee”. Иногда, когда адрес кажется подлинным, можно увидеть, что строка получателя полностью отличается от отправителя при ответе на сообщение.

2. В случае с веб-сайтами надо смотреть на адрес ссылки. Как и в случае с адресами электронной почты, адрес веб-страницы также может быть изменен, например, адрес оканчивается на “.ea” вместо “.ee” или к адресу добавляются цифры для замены букв, например “eest1.ee” вместо “eesti.ee”.
3. Электронные письма и веб-сайты, которые обещают деньги, путешествия, бесплатные вещи и т. д., скорее всего, являются мошенническими.
4. Поскольку киберпреступники обычно из других стран, электронная почта или веб-страница часто переводятся на эстонский, русский или английский язык переводчиком Google или аналогичной программой и поэтому могут содержать значительное количество грамматических или стилевых ошибок. Поскольку киберпреступники постоянно развиваются, а программы перевода становятся все лучше, нельзя слепо доверять электронной почте или веб-сайту, написанному на корректном эстонском, русском или английском языке.
5. Если электронное письмо приходит от руководства организации или бухгалтера, следует проверить, соответствует ли электронное письмо обычному стилю, особенно при требовании перевода денег. Мошеннические письма, как правило, подозрительно короткие и в приказном тоне (например, «Оплати сейчас, его нужно оплатить в течение 24 часов!» и т. д.).

4.2 Обучайте работников

В дополнение к повышению общей осведомленности о кибербезопасности среди сотрудников, следует обеспечить и направленное обучение пользователей. Такое обучение должно охватывать вопросы безопасности в более широком смысле: поведение в социальных сетях, использование открытых облачных сервисов, безопасное использование WiFi и т. д.

План обучения может включать в себя:

1) ознакомление с правилами информационной безопасности компании, объяснение требований безопасности и рисков;
2) анализ рисков различных устройств и сервисов (портативные устройства, социальные сети, открытые облачные сервисы и т. д.)
3) поведение в случае инцидентов безопасности (кому сообщать, что делать и т. д.);
4) выявление потенциальных угроз и наиболее распространенных типов атак, оценка последствий таких атак;
5) анализ последних инцидентов безопасности, которые были обнародованы, с описанием причин и возможных превентивных мер.

4.3 Регулярно проверяйте знания сотрудников

Для проверки эффективности обучения, а также для установления уровня знаний сотрудников, последние должны регулярно проверяться. Это поможет сотрудникам вспомнить, что они узнали, и сохранять это в памяти. Знания могут быть проверены, например, с помощью опросов, которые могут быть предоставлены различными службами кибербезопасности или обучающими компаниями, которые лучше всего могут

их составить и своевременно обновлять. Это также предоставит компании информацию о том, требует ли какая-то тема повторного обучения.

Также полезно выполнять небольшие упражнения для проверки поведения сотрудников - например, отправлять поддельные фишинговые письма сотрудникам. Результаты таких тестов подскажут вам, что еще нужно рассказать пользователям или нужно ли дополнительное обучение.

5 Учитесь восстанавливать

Иногда возникают ситуации, когда данные (файлы, электронные письма, базы данных и т. д.) теряются или портятся. Это может быть связано с тем, что сотрудник случайно удаляет некоторые файлы или перезаписывает файл с неверными данными. Кроме того, существуют кибератаки (например, криптовирусы), кража оборудования или аварии (пожар, наводнение), которые разрушают или портят данные. Поэтому важно, чтобы все данные, важные для компании, постоянно сохранялись и резервные копии хранились в безопасном месте.

Полезно знать!

Программа-вымогатель - это вирус, который шифрует все или некоторые данные на компьютере или сервере, что делает их непригодными для использования. Чтобы файлы снова стали пригодными для использования, злоумышленникам надо заплатить деньги.

5.1 Создайте план восстановления

Очень важно создать план восстановления. Хотя может показаться, что известно, как система будет восстановлена в случае сбоя, закон Мерфи предполагает, что необходимость восстановления информационной системы может возникнуть в самые загруженные часы работы организации, и когда недоступен специалист по восстановлению системы. В этом случае план восстановления поможет в наиболее критических ситуациях быстро и правильно восстановить систему. План восстановления подробно описывает, шаг за шагом, этапы, которые специалист должен выполнить для восстановления системы.

План восстановления должен детально предоставить всю информацию, необходимую для восстановления систем, важных для компании:

1) описание аппаратного и программного обеспечения - все оборудование, инструменты, данные и версии программного обеспечения, необходимые для восстановления, и их точное местоположение;
2) пошаговое руководство - какие действия предпринять в каком порядке;
3) системные настройки для восстановления;
4) пользователи, необходимые для восстановления (учетные записи, пароль администратора и т. д.).

5.2 Резервное копирование и контроль

При планировании резервного копирования сначала необходимо определить, какие данные важны для компании и для каких необходимо выполнить резервное копирование. Необходимо выполнить резервное копирование всей важной информации - электронной почты, баз данных программного обеспечения для бизнеса, общих каталогов и файлов, и следует также учитывать данные на компьютерах пользователей.

Во-вторых, вам нужно подумать о том, насколько старые данные можно будет в состоянии восстановить из резервной копии. Возможно для важных данных, таких как общая папка или программное обеспечение для бизнеса, резервное копирование надо делать

ежедневно, и хранить, например, только один месяц (то есть возможно будет восстановить данные за один месяц). Для данных, которые меняются нечасто (например, банк фотографий или архив), можно создавать резервные копии раз в месяц и хранить только одну копию.

Спросите у IT специалиста!

Обратитесь к своему IT специалисту или поставщику услуг для организации резервного копирования (какие данные, частота, количество резервных копий).

Чтобы защитить резервную копию в случае аварии (пожара, наводнения) или кражи, следует также создать внешнюю резервную копию. Эта резервная копия может находиться в облаке, в другом офисе или, например, у хостинг-провайдера. В этом случае, если ваши устройства и данные будут потеряны, внешняя резервная копия находится в безопасном месте. В случае облачной службы или стороннего поставщика услуг следует иметь в виду, что данные находятся у кого-то другого, и следует подумать о том, надо ли хранить резервные копии конфиденциальных данных и коммерческой тайны у них.

Также важно убедиться, что резервная копия будет в рабочем состоянии, потому что невозможно восстановить данные из поврежденной резервной копии. Для этого необходимо настроить уведомление по электронной почте о том, насколько хорошо работает резервное копирование, и регулярно проверять журналы резервного копирования, чтобы убедиться, что копии были успешными. Имеет смысл периодически проверять, что все необходимые данные копируются (например, папка могла быть перемещена в другое место и не сохранена) и, при необходимости, изменить параметры резервного копирования. Кроме того, важно вести учет резервного копирования: какие данные и куда сохраняются, сколько записей хранится, какая программа занимается резервным копированием и т. д.

5.3 Делайте пробные восстановления

Очень важно регулярно делать тестовые пробные восстановления. Во время этих операций некоторые важные части системы восстанавливают в изолированном от текущей системы месте (чтобы это не влияло на рабочую среду) и проверяют, все ли работает после восстановления. Пробные восстановления важны, потому что даже если резервные копии кажутся успешными, могут быть непредсказуемые ошибки восстановления системы. Например, резервная копия может быть неисправна, данные могут отсутствовать или могут потребоваться дополнительные настройки для восстановления системы. Любые обнаруженные отклонения и специальные настройки должны быть задокументированы в плане восстановления. Пробные восстановления должны быть сделаны для всех важных систем, и для резервного копированиядолжна быть произведена случайная выборка.

Спросите у IT специалиста!

Узнайте у своего IT специалиста или поставщика услуг, существует ли план восстановления для восстановления систем вашей организации и были ли выполнены пробные восстановления. При необходимости следует создать план восстановления и организовать пробное восстановление.

6 Защищайте свою торговую марку

Общедоступные веб-сайты, учетные записи социальных сетей и адреса электронной почты связаны с товарным знаком компании. Поскольку они общедоступны, существует риск того, что злоумышленники захотят использовать их, чтобы нанести ущерб репутации компании, заработать деньги или по другим причинам. Поэтому важно, чтобы они были защищены.

6.1 Держите себя в курсе потенциальных опасностей

Государственные службы (веб-сайты, электронная почта) подвержены угрозам, которые могут нарушить работу организации и нанести ущерб репутации компании.

Связанные с общедоступным веб-сайтам риски могут быть следующие:

1. Злоумышленники могут сделать сайт компании недоступным Это, например, парализует работу компании, занимающейся электронной коммерцией, а также мешает работе многих других компаний, поскольку клиенты могут не получать необходимую им информацию с веб-сайта.
2. Злоумышленники могут получить доступ к управлению веб-сайтом и украсть информацию, например, о корпоративных клиентах, что может привести к ущербу для репутации и штрафам GDPR.
3. Злоумышленники могут сделать содержание сайта неуместным (например, оскорбительным), что опять-таки может подорвать работу организации и нанести ущерб её репутации.
4. Злоумышленники могут установить на веб-сайт программное обеспечение, которое будет заражать клиентов, посещающих веб-сайт, вредоносными программами. Это приводит к ситуации, когда клиенты компании начинают избегать этого сайта, даже когда он будет исправлен.

Полезно знать!

Общее положение о защите данных (GDPR (General Data Protection Regulation)) - это Европейское общее положение о защите данных, устанавливающее руководящие принципы обработки персональных данных в Европейском союзе. Нарушение GDPR может привести к крупным штрафам: 20 000 000 евро, или 4% от оборота предыдущего года, в зависимости от того, что больше. Более подробная информация: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_et.

Если злоумышленники завладеют учетными записями в социальных сетях, это может испортить репутацию (неуместные публикации, оскорбление клиентов и т. д.), так и вызвать финансовые убытки компании, если эти учетные записи связаны с платежами (например, злоумышленники могут получить доступ к кредитной карте, которая привязана к покупкам рекламы на Facebook). Следует иметь в виду, что в дополнение к собственным учетным записям в социальных сетях необходимо защищать учетные записи руководства и ключевых сотрудников компании.

Если служба рабочей электронной почты не защищена, злоумышленники могут использовать адреса электронной почты компании для мошенничества или рассылки спама. Это может испортить репутацию, так и вызвать финансовые убытки компании.

6.2 Защитите себя от угроз

Первым шагом в защите от угроз является понимание того, что они существуют. Для защиты от угроз компании могут предпринять ряд мер по их предотвращению.

6.2.1 Выберите инструменты для обнаружения уязвимостей в безопасности

Для атаки на общедоступную службу обычно используются уязвимые места в защите программного обеспечения службы (например, веб-сайта или сервера электронной почты), слабые настройки безопасности, неизмененные пароли и т.д. Существуют различные инструменты для обнаружения уязвимостей, которые делают это автоматически. Такие инструменты сканируют публичные сервисы и генерируют исчерпывающие отчеты об обнаруженных уязвимостях. После обнаружения они должны быть удалены IT персоналом или поставщиком услуг. Затем следует выполнить новое сканирование, чтобы увидеть, были ли устранены ранее обнаруженные уязвимости в системе безопасности. Их необходимо регулярно проверять (например, раз в месяц), чтобы последовательно обнаруживать и устранять новые уязвимые места в безопасности.

Спросите у IT специалиста!

Существуют различные решения для обнаружения уязвимостей в безопасности. Узнайте у своего IT персонала или поставщика услуг соответствующее программное обеспечение.

6.2.2 Защитите ваши общественные услуги

Обнаруженные уязвимости безопасности необходимо устранить, чтобы защитить публичные сервисы. Также важно, чтобы программное обеспечение веб-сервера или почтового сервера было обновлено (см. 2.2 “Регулярно обновляйте программное обеспечение”). Обновлять надо как сервер службы так и само программное обеспечение службы.

Спросите у IT специалиста!

Если сервер размещен и управляется вашим поставщиком услуг, следует проверить у него, регулярно ли обновляется программное обеспечение сервера.

Для защиты службы электронной почты, ваш IT персонал или поставщик услуг должен установить следующие параметры:

1. Чтобы запретить злоумышленникам свободно использовать корпоративные адреса электронной почты, необходимо в DNS создать запись SPF (Sender Policy Framework), которая сообщает, какие серверы электронной почты могут отправлять почту с вашего корпоративного почтового домена.

2. Также можно настроить DKIM (DomainKeys Identified Mail) для проверки правильности работы корпоративного почтового сервера. DKIM подписывает исходящие электронные письма с сервера, а другие почтовые серверы проверяют правильность подписи. Чтобы иметь возможность использовать DKIM, корпоративный почтовый сервер должен поддерживать эту услугу, или необходимо приобрести или установить дополнительное программное обеспечение
3. DMARC (Domain-based Message Authentication, Reporting and Conformance) через DNS распространяет на серверы электронной почты политику, в которой говорится, что следует проверять в отправленных с этого домена сообщениях, и как сервер электронной почты должен обрабатывать это сообщение. DMARC использует SPF и DKIM для проверки соответствия своим политикам. DMARC может использоваться только с SPF, но более безопасный режим обеспечивается при использовании DKIM. С помощью DMARC можно получать отчет о том, пытался ли кто-либо отправлять почту из других мест, кроме тех, которые разрешены.

6.2.3 Защищайте свои учетные записи в социальных сетях

Корпоративные социальные сети, такие как Twitter, Facebook, Instagram и т. д., часто подвергаются атакам. Учетные записи руководства и ключевых сотрудников компании также подвергаются риску и должны быть защищены.

Для защиты учетных записей социальных сетей организации необходимы следующие шаги, которые совсем не сложны, но значительно повышают безопасность:

1. Создайте правило использования корпоративных социальных сетей (какой сотрудник может получить доступ к какой учетной записи, какие учетные записи используются, какой сотрудник ими управляет, как он ведет себя в социальных сетях и т. д.).
2. Используйте надежные пароли!
3. Регулярно меняйте свои пароли. Обязательно надо изменить пароли, когда сотрудник, который получал доступ к этой учетной записи, покидает компанию.
4. Обязательно включите многоэтапную аутентификацию.
5. Время от времени проверяйте существующие учетные записи в социальных сетях. Контролируйте, кто может получать доступ к аккаунтам и удаляйте его у людей, покинувших компанию, и у тех, кому он уже не нужен.
6. Кроме того, проверяйте настройки учетной записи, поскольку параметры конфиденциальности могут изменяться по мере обновления социальных сетей или может меняться закон (например, до этого личная информация теперь может быть доступна всем).
7. Если учетные записи не используются активно, их все равно следует отслеживать на предмет возможного захвата учетных записей.

Спросите у IT специалиста!

Если организация активна в социальных сетях, то можно рассмотреть возможность использования программного решения, предназначенного для защиты учетных записей в социальных сетях. Например, оно позволяет автоматически удалять подозрительный контент, предотвращать публикацию недопустимого контента, обнаруживать другие учетные записи, созданные под брендом компании, и так далее. Спросите у своего IT специалиста или поставщика услуг о таких решениях.

Что делать, если произошел кибер инцидент?

- Постарайтесь как можно быстрее понять причины и источник инцидента, чтобы остановить его и минимизировать ущерб.
- Оповестите своих сотрудников об инциденте.
- Сообщите об инциденте своим клиентам или партнерам, кого он затронул.
- Информируйте Отдел обработки инцидентов RIA CERT-EE (cert@cert.ee).
- Подумайте, нужно ли сообщать об инциденте в полицию и / или Комиссию по защите личных данных.
- Информируйте ваших сотрудников, клиентов (и, если применимо, широкую общественность) о том, как восстанавливается инцидент.