Тезисы по безопасности хранения корпоративных баз данных.

У нас довольно большой и длительный опыт работы в сфере сопровождения серверов Заказчиков, а также предоставления облачных сервисов через интернет. Мы подготовили для Вас в сжатом виде тезисы, базирующиеся на нашем опыте, по безопасности и некоторые рекомендации.

1. Угрозы внешних атак

В текущей сложной ситуации данный аспект безопасности особенно актуален.

При решении данного вопроса есть ряд сложностей. С одной стороны, размещая базы 1С в облаке, вы заведомо знаете, что высококвалифицированные специалисты постарались обеспечить максимальную безопасность ваших данных и защититься от взлома. С другой стороны, популярные и известные облачные сервисы привлекают больше внимания со стороны злоумышленников и, соответственно, попыток атак на них значительно больше, чем возможно будет у вас на вашем оборудовании. Конечно, размещая базы 1С у себя, вы можете надеяться на компетенции вашего IT специалиста и на то, что о ваших серверах

никто в интернете не знает.

Но наш опыт подсказывает, что 100% защиты от внешних атак не существует. Любое устройство, подключенное к интернету, сканируется автоматическими системами злоумышленников на уязвимости и, как результат, риск есть всегда.

Что мы рекомендуем для минимизации рисков от внешних атак:

- Сделать так, чтобы об внешних ip адресах, где размещается Ваша база данных, знали как можно меньше сторонних сервисов и как можно меньший круг людей. Важно, если базы опубликованы в интернет, обеспечить, чтобы на индексируемых сайтах не было ссылок на Ваши базы данных.
- Если есть возможность, обеспечить доступ к базам данных только через VPN.
- По возможности хранить в рабочих базах данных 1С такую информацию, даже заполучив которую, злоумышленники не смогут нанести большого вреда деятельности компании.
- И самое главное - настроить систему резервирования ваших данных таким образом, чтобы даже если взлом произойдет, у вас всегда были резервные копии для обеспечения возможности дальнейшей работы компании.

2. Безопасность утечки информации

По нашему опыту наибольшую угрозу в данном аспекте представляют внутренние сотрудники компании, знакомые с принципами получения прибыли компании и технологией ее работы.

Наиболее часто такие угрозы возникают в небольших компаниях с высокой маржинальностью единичной сделки. В этих компаниях сотрудники обладают глубокими знаниями о клиентской базе и бизнес-процессах, что увеличивает вероятность злоупотребления.

В результате возникают ситуации, когда сотрудники компании «уносят» базу CRM клиентов с персональными данными ЛПР, историей взаимодействий и предстоящими сделками, что создает значительные риски для бизнеса.

Первый шаг к минимизации рисков — ограничение доступа к базам данных 1С. Это означает, что сотрудники компании не должны иметь доступ к физическому размещению баз данных сами, ни через других сотрудников, даже запросив у IT-администратора. Желательно, чтобы такой доступ был только у учредителей или у очень ограниченного круга лиц.

Решить данную задачу возможно в несколько этапов:

1. Разместить базы 1С на оборудовании, которое физически не находится на территории заказчика.
2. Передать оборудование во внешнее сопровождение компании, где их собственные специалисты, во-первых, не имеют никакого представления о технологиях работы вашей организации, и во-вторых, несут уже более высокую ответственность за безопасность ваших данных. Это связано с тем, что аутсорсинговые компании сопровождают множество организаций, берегут свою репутацию и заключают соответствующие юридически значимые соглашения со своими сотрудниками.

Как результат, размещение базы 1С в каком-либо облачном сервисе позволит закрыть данный вопрос на 50%. Оставшиеся 50% — это уже разграничения прав доступа в самой базе данных. Хоть внутренние сотрудники или злоумышленники уже не смогут быстро украсть всю базу данных, остается возможность распечатать, переписать данные, если к ним есть доступ в пользовательском режиме.

3. Угрозы потери данных

Многие руководители считают, что для того чтобы обеспечить безопасность хранения данных, достаточно купить сервер с резервированием дисков подороже и можно не беспокоиться о сохранности. Наш опыт говорит, что этого совсем не достаточно. Довольно много компаний к нам обращались с очень типичной ситуацией: RAID массив, на котором находились все данные заказчика, терялся по причине поломки оборудования контроллера или потери последнего работающего диска в массиве.

Исследование данного вопроса показало, что без организации качественной IT поддержки ваших серверов покупка дорогостоящих систем резервирования бесполезна. Ведь, если никто не анализирует информацию о состоянии оборудования, дисков на серверах, если никто не проверяет, что резервные копии баз 1С сохранились и продолжают сохраняться, то нельзя быть уверенным в том, что вы не потеряете все свои данные. Любое оборудование ломается со временем, и без надлежащего контроля риск потерять данные повышается.

Рекомендации:

Закрыть эту угрозу довольно легко. Необходимо или организовать собственный отдел IT, или заключить договор со сторонней компанией на обслуживание, где все эти моменты будут прописаны.

Размещение же ваших баз в облаке 1С в датацентре позволит закрыть данный вопрос значительно дешевле, поскольку все эти услуги и мероприятия по безопасности уже входят в стоимость облачных решений. Очевидно, что облачные провайдеры изначально содержат штат высококвалифицированных IT специалистов, которые обеспечивают надежную работу множества организаций.

4. Угрозы от вирусов-шифровальщиков

Угроза заражения сети вирусом-шифровальщиком в любой компании довольно высока, и она тем выше, чем больше компьютеров находится в сети и чем больше сотрудников работает в компании.

Чем определяется данная угроза:

- Ваши сотрудники не обязаны все быть специалистами в области IT, поэтому высок риск того, что они неосознанно могут запустить неизвестный файл из почты или флешки с вирусом, о котором не знает ваша антивирусная программа.
- Большая часть вирусов-шифровальщиков написана под Windows. В большинстве компаний зачастую на ОС Windows работают не только пользователи, но и серверное оборудование и даже компьютеры, на которые производится резервирование данных.

Рекомендации:

Значительно обезопасить корпоративные данные от вирусов-шифровальщиков можно, используя операционную систему, для которой существует еще не так много вирусов, например Linux. Конечно, на сегодняшний день существуют вирусы и под Linux, но их гораздо меньше, и заразить сервер на Linux будет значительно сложнее, даже если все компьютеры в офисе будут заражены. Ведь вирусы для этих ОС разные.

У облачных провайдеров 1С на сегодняшний день большая часть серверов работает на Linux, поскольку это позволяет не только повысить безопасность, но и снизить стоимость предоставляемых услуг.

Также полезной рекомендацией будет периодическое обучение сотрудников на тему безопасности работы в интернет и с электронной почтой.

Revision #7
Created 26 April 2023 11:42:21 by Евгений Гордеев
Updated 6 November 2024 08:49:49 by Евгений Гордеев