ЦЕНТРЫ ОБРАБОТКИ ДАННЫХ (ЦОД)

Курс лекций

Лекция 17. Система информационной безопасности ЦОД

Общие особенности ЦОД, как объекта защиты информации

Для крупных коммерческих ЦОД характерны:

- концентрация больших вычислительных мощностей в ограниченном пространстве;
- обслуживание большого количества клиентов, приложений, бизнес-процессов;
- совместная обработка в одной программно-аппаратной среде информации разного характера — открытой информации, персональных данных, информации, содержащей коммерческую тайну и т. п.

Основные риски, приводящие к наиболее тяжелым последствиям:

- приостановка деятельности ЦОД;
- масштабное хищение или модификация информации за счет внешнего или внутреннего взлома.

Отсутствует нормативная база, регулирующая:

- соответствие ЦОД требованиям к размещению и обработке информации разной категории;
- обязательства перед клиентами по сохранению размещаемой клиентами информации;
- соблюдение требований федеральных законов, в том числе и закона “О персональных данных”.

Большая роль фактора доверия, вытекающая из отсутствия:

- нормативной базы;
- методов сертификации процессов оказания услуг;
- требований к инфраструктуре провайдера и владельца ЦОД.

Технологические особенности ЦОД и защита информации

- Широкое использование виртуальной среды, т.е. размывание границ нахождения информации.

На одном физическом сервере может размещаться информация разных уровней конфиденциальности, например, интернет-сегменты виртуальных машин и базы данных (БД). Разделение коммуникаций – только через гипервизор.

Отсюда возможность :

- удаленного несанкционированного доступа к особо защищаемым данным, хранящимся в, например, в БД;
- удаленного внесения изменения в архитектуру системы виртуализации путем воздействия на гипервизор;
- повреждение гипервизора или средств защиты информации, установленных на виртуальных серверах.

Способы борьбы:

- размещение средств защиты (межсетевых экранов, систем обнаружения и предотвращения вторжений, контроля целостности, анализа журналов и т.д.) непосредственно на серверах виртуализации;
- использование программных средств контроля целостности гипервизора;
- сегментирование ресурсов по степени критичности обрабатываемой информации и применение мер защиты как на границах сегментов, так и внутри них.

- Каналы передачи данных подконтрольны не владельцу ЦОД, а компании-провайдеру.

Между заказчиком и исполнителем находится третье лицо, обязанности которого строго не определены.

Способы борьбы:

- тщательное составление и контроль SLA (Service Level Agreement) - соглашения об уровне сервиса с провайдером;
- требования к провайдеру о переходе от принципа «делаю, что могу» к принципу «делаю, как требуют»;
- предоставление владельцем ЦОД услуг провайдера.

- Высокие требования к производительности средств защиты.

Сложные системы защиты информации влияют на производительность серверного оборудования ЦОД.

Способ борьбы:

- перенос нагрузки, связанной с защитой информации, на выделенные серверы;

- Требования по СОРМ (системе организационно-розыскных мероприятий).

Из-за претензий к одному клиенту ЦОД доступа к сервисам могут быть лишены и другие (например, в случае изъятия жестких дисков).

Способ борьбы:

- аренда выделенных серверов (collocation);
- использование ЦОД, размещенных за рубежом.

Специфика угроз информационной безопасности в ЦОД

Цель атак:

- получение ценной информации из БД клиентов ЦОД;
- остановка работы ЦОД и тем самым нанесение ущерба репутации его владельца или пользователя;
- завладение удаленным управлением, для изменения внутренних процессов систем.

Возможные механизмы:

- Использование уязвимостей в системе разграничения доступа - легальная аренда виртуальной площадки, с которой осуществляется проникновение в другие информационные системы.
- DDoS-атака (Distributed Denial of Service) - распределённая атака типа «отказ в обслуживании» производится с многих компьютеров с целью довести вычислительную систему до такого состояния, при котором легитимные пользователи не могут получить доступ к ресурсам (серверам). Обычно это мера экономического давления на провайдера ввиду нарушения SLA (Service Level Agreement) - соглашения об уровне сервиса.
- Человеческий фактор – инсайдеры из ЦОДа, непреднамеренные ошибки персонала.

Способы борьбы с угрозами

Межсетевые экраны - комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Основной задачей межсетевого экрана является защита компьютерных сетей или их отдельных узлов от несанкционированного доступа.

Средства обнаружения и предотвращения вторжений (IDS/IPS - Intrusion detection system/Intrusion prevention system) – программные и аппаратные средства для обнаружения и предотвращения вторжений, предназначенные для обнаружения и предотвращения попыток несанкционированного доступа и используемые для обнаружения аномальных действий в сети, которые могут нарушить безопасность и конфиденциальность данных (попытки использования уязвимостей ПО, повышения привилегий, несанкционированного доступа к конфиденциальным данным, активности вредоносного ПО - вирусов, троянов, червей и т.д.). IDS/IPS пропускает трафик, анализируя его и сигнализируя при обнаружении подозрительной активности.

Антивирусная защита – средства защиты от вирусов различных типов, которые могут быть внедрены в систему для дезорганизации ее работы.

VPN (Virtual Private Networks) – виртуальные частные сети – программные и аппаратные средства шифрования трафика.

Административные меры – программы повышения лояльности сотрудников, правильное разграничение доступа, контроль использования критически важных систем несколькими сотрудниками с различным уровнем прав (за назначение прав доступа к защищаемым ресурсам клиентов ЦОД должен отвечать администратор безопасности, который, в свою очередь, не получает прав доступа к самим ресурсам).

Безопасность инженерных систем

Долгое время при создании ЦОД основное внимание уделялось безопасности корпоративного периметра (сетевое оборудование, серверы), а инженерная инфраструктура (контроллеры, ИБП и т.д.) оставалась в стороне. Эти устройства могут быть выделены в отдельную сеть или находиться в одной сети с прочим оборудованием. Часть оборудования (чиллеры и управляющие ими контроллеры) обычно вынесена на крышу здания. Служба безопасности обычно не наблюдает за ними, а эксплуатирующие эти установки специалисты не занимаются вопросами безопасности. При этом сеть часто не сегментирована, не меняются пароли и не используются средства защиты. Это может быть опасно.

Поскольку злоумышленник практически всегда идет по пути наименьшего сопротивления, одной из возможных целей атаки может стать атака на инженерную инфраструктуру. Практически никто из владельцев ЦОД не уделяет достаточного внимания защите этих систем. Сейчас ситуация меняется, и владельцам ЦОД приходится задумываться о безопасности инженерных систем для противостояния угрозам.

Безопасность инженерных систем

Должны быть приняты меры:

- организационные меры;
- обеспечения безопасности периметра инфраструктуры инженерных систем и сети управления ими;
- проверки сети на наличие посторонних узлов;
- контроля наличия необходимых средств аутентификации и авторизации;
- мониторинг сетевой активности.

Проблема актуальна для России, поскольку часто построенный по грамотному проекту ЦОД уже через пару лет представляет собой нечто менее упорядоченное и продуктивное, чем планировалось. Культура эксплуатации в России очень медленно развивается, и специалистов для долгосрочной эксплуатации не хватает. Более того, не хватает менеджеров, которые знают, как построить работу ЦОД в долгосрочной перспективе.

Социальная инженерия и ИБ

Самое слабое звено в системе обеспечения безопасности ЦОД — это люди.

Социальная инженерия - метод несанкционированного доступа к информации или системам ее хранения без использования технических средств. Метод основан на использовании слабостей человеческого фактора и является очень эффективным. Применительно к ЦОД это означает, что злоумышленник получает информацию, например, путем сбора информации о служащих ЦОД с помощью обычного телефонного звонка. Злоумышленник может позвонить сотруднику ЦОД под видом работника технической службы и выведать пароль, сославшись на необходимость решения небольшой технической проблемы в системе. Все техники социальной инженерии основаны на особенностях принятия решений людьми.

Техники социальной инженерии

Среди техник социальной инженерии можно выделить следующие:

- *Претекстинг* — действие, отработанное по заранее составленному сценарию (претексту). Жертва должна выдать определённую информацию, или совершить определённое действие Применяется обычно по телефону и обычно требует каких-либо предварительных исследований (например, персонализации: выяснение имени сотрудника ЦОД, занимаемой им должности и выполняемых им служебных обязанностей), с тем, чтобы обеспечить доверие цели.
- *Фишинг* — злоумышленник посылает сотруднику ЦОД e-mail, подделанный под руководящее указание «проверки» определённой информации, или совершения определённых действий. Обычно содержит ссылку на фальшивую web-страницу, имитирующую официальную, с корпоративным логотипом и содержащую форму, требующую ввести конфиденциальную информацию.
- *Троянский конь* - техника эксплуатирующая любопытство, либо алчность цели. Злоумышленник отправляет e-mail, содержащий во вложении важное обновление антивируса, или даже свежий компромат на сотрудника. Такая техника остаётся эффективной, пока пользователи будут слепо кликать по любым вложениям.

Техники социальной инженерии

Дорожное яблоко - метод атаки, представляющий собой адаптацию троянского коня, и состоящий в использовании физических носителей. Злоумышленник может подбросить инфицированный CD, или карту памяти, в месте, где носитель может быть легко найден (коридор, лифт, парковка). Носитель подделывается под официальный, и сопровождается подписью, призванной вызвать любопытство.

Кви про кво - злоумышленник может позвонить по случайному номеру сотруднику ЦОД, и представиться сотрудником техподдержки, опрашивающим, есть ли какие-либо технические проблемы. В случае, если они есть, в процессе их «решения» сотрудник вводит команды, которые позволяют злоумышленнику запустить вредоносное ПО.

Обратная социальная инженерия – попытка заставить сотрудника ЦОД самому обратиться к злоумышленнику за «помощью». С этой целью злоумышленник может применить технику диверсии, т.е. создать обратимую неполадку на компьютере жертвы и выдавая себя за сотрудника техподдержки предложить услуги по ее устранению.

Способы защиты от социальной инженерии и противодействие инсайду

Способы защиты от социальной инженерии:

- обучение; все сотрудники ЦОД должны знать об опасности раскрытия информации и способах ее предотвращения;
- сотрудники ЦОД должны иметь четкие инструкции о том, как, на какие темы говорить с собеседником, какую информацию для точной аутентификации собеседника им необходимо у него получить;
- введение должности администратора виртуальной инфраструктуры, что повышает значимость противодействия как злонамеренному инсайду, так и непреднамеренным ошибкам со стороны этих специалистов.

Противодействие инсайду:

- правильное разграничение доступа к ресурсам, исключение единоличного доступа специалистов к критически важным системам;
- жесткая политика информационной безопасности, обязывающая привлекать к контролю использования таких систем нескольких сотрудников с различным уровнем прав, а также тщательный контроль исполнения политик.

Противодействие инсайду

- разделение ролей и сфер ответственности; например, за назначение прав доступа к защищаемым ресурсам клиентов ЦОД должен отвечать администратор безопасности, который, в свою очередь, не получает прав доступа к самим ресурсам;
- максимальное исключение из функционирования системы информационной безопасности ЦОД человеческого фактора;
- централизация управления средствами защиты информации, например, устанавливать и настраивать межсетевой экран администратору гораздо удобнее и быстрее со своего рабочего места, чем на каждом объекте в отдельности.

На создание и обеспечение функционирования ЦОД тратятся огромные финансовые средства, как и на обеспечение ЦОД информационной безопасности техническими методами. Однако эти технические средства могут быть обойдены, если сотрудники ЦОД не будут применять меры по противодействию социальным инженерам, а службы безопасности не будут периодически проводить обучение персонала, проверять его бдительность и умение пользования инструкциями и наставлениями.

Нормативная база ИБ

Федеральный закон от 27 июля 2006 года N 152-ФЗ “О персональных данных”.

Даже в последней редакции закона отсутствуют регламенты использования виртуализации и облачных вычислений с позиций ИБ. Это создает проблемы потребителям услуг ЦОД, которым необходимы закрепленные договором обязательства по соблюдению в отношении размещаемой клиентами информации требований федеральных законов, включая закон “О персональных данных”. В настоящее время типовой договор провайдеров предполагает предоставление услуг “как есть”, что переносит все риски, связанные с защитой информации на потребителей услуг. Это обстоятельство заметно сдерживает развитие рынка коммерческих ЦОД, поскольку они эксплуатируются разными юридическими лицами и разрешение некоторых вопросов информационной безопасности могут вызвать юридические проблемы и создать конфликтные ситуации. Это останавливает значительное число потенциальных потребителей услуг ЦОД, которые предпочитают создавать свои, не всегда совершенные ЦОД, не прибегая к услугам коммерческих.

Нормативная база ИБ

Федеральный закон № 187 от 26.07.2017 «О безопасности критической информационной структуры Российской Федерации».

Регулирует безопасность объектов критической информационной инфраструктуры (КИИ). Законом определяются субъекты КИИ, куда входят как любые организации, которые владеют на законных основаниях такими объектами, так телекоммуникационные сети, автоматизированные системы управления и информационные системы в отраслях топливно-энергетического комплекса, в области атомной энергетики, в финансовом секторе, энергетике, транспорте и т. д. Сфера применения закона достаточно велика.

Постановление Правительства РФ от 19 октября 2017 г. N 1273 «Об утверждении требований к антитеррористической защищенности торговых объектов (территорий) и формы паспорта безопасности торгового объекта (территории)».

Указаны критерии значимости для оценки этих объектов в соответствии с требованиями ФСТЭК - Федеральной службы по техническому и экспортному контролю Оцениваются потенциальные последствия инцидента безопасности (гибель людей, нарушение предоставления определенных сервисов, ущерб экологии и т.д.) В зависимости от величины потенциального ущерба присваивается либо не присваивается одна из трех категорий значимости. В зависимости от категории значимости реализуется соответствующий комплекс мер по защите данных объектов.

Фактор доверия и ИБ в ЦОД

Отсутствие нормативного регулирования защиты информации в ЦОД увеличивает роль фактора доверия в отношениях между провайдерами и клиентами. Эти отношения во многом зависят от того, насколько тщательно поставщик услуг предусмотрел различные аспекты обеспечения информационной безопасности и заложил их в свою систему. Трудности, связанные с обеспечением информационной безопасности, провайдеры зачастую стараются переадресовывать самим клиентам, если предоставляемые им ресурсы допускают доработку систем провайдеров под их требования. Поэтому следует максимально внимательно оценивать поставщика услуг и договор с ним.

В настоящее время доля использования коммерческих ЦОД в ИТ-проектах начинает вытеснять собственные площадки. Для этого есть ряд причин: более высокий уровень маштабируемости, быстрый для клиента запуск ИТ-решений, круглосуточно доступный компетентный персонал и другие преимущества, реализовать которые самостоятельно сложнее и дороже. Все зависит от степени готовности клиента делегировать оператору ЦОД определенные задачи, в том числе, в области обеспечения информационной безопасности. В настоящее время на российском рынке уже появляются даже сертифицированные продукты, с помощью которых можно реализовать контроль исполнения политики безопасности клиента. Свою положительную роль играет и сертификация ЦОД по уровню стабильности работы, включающая вопросы информационной безопасности.

Решения российских компаний по обеспечению ИБ в ЦОД

Компания **«Код Безопасности»** - российский разработчик сертифицированных средств защиты информации.

Продукты компании обеспечивают защиту конечных станций и серверов, периметра сети, современных виртуальных инфраструктур и мобильных устройств сотрудников.

При решении задачи защиты ЦОД необходимо учесть два основных фактора:

- защита сетевой инфраструктуры;
- защита конечных точек.

Для защиты сетевой инфраструктуры используются многофункциональные межсетевые экраны. Для решения задачи защиты серверов - связка из таких продуктов компании, как решение для защиты рабочих станций и серверов «Secret Net Studio» и сертифицированный аппаратно-программный модуль доверенной загрузки (АПМДЗ) «СОБОЛЬ».

Решения российских компаний по обеспечению ИБ в ЦОД

Компания **АО «РНТ»** - разработчик систем обнаружения и предотвращения компьютерных атак нового поколения на базе распределенной системы мониторинга и управления «Форпост-мониторинг».

СОА «Форпост» 3.0 имеет характеристики:

- скорость обработки сетевого трафика - до 10 Гб/с;
- встроенные механизмы защиты - В соответствии с требованиями ФСТЭК и ФСБ России;
- интерфейс - web-интерфейс, карта сети, интерактивные интерфейсы устройств;
- интеграция - все отечественные и ведущие мировые системы;
- сертификаты - В процессе сертификации: ФСТЭК - 2 и 4 классы защиты, ФСБ - класс Б;
- возможность работы в виртуальных средах – да в том числе создание виртуальных устройств.