УДК: 004.056:004.91

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ФИЗИЧЕСКАЯ ЗАЩИТА ЦЕНТРА ОБРАБОТКИ ДАННЫХ

Матюшин Дмитрий Сергеевич, *магистрант группы ИТССм-1-16, направления 690300-Инфокоммуникационные технологии и системы связи, КГТУ им. И.Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Мира 66, e-mail: dmitriy.matyushin@m-vector.com*
Абдыллаева Гульнара Оморовна, *к.п.н., доцент, КГТУ им. И.Раззакова, Кыргызстан, 720044, г. Бишкек, пр. Мира 66, e-mail: g.abdyllaeva@mail.ru*

Цель статьи: Рассмотрение вопросов информационной безопасности и физической защиты

Центра обработки данных, в том числе жестких требований к информационной безопасности при обеспечении прозрачного доступа клиентам через сеть Интернет, а так же вероятность утечки информации.

Ключевые слова: Центр обработки данных, информационная безопасность, сеть Интернет, защита информации, утечка информации.

INFORMATION SECURITY AND PHYSICAL PROTECTION OF DATA CENTER

Matyushin Dmitriy Sergeevich, *graduate student of IET under the KSTU named after I. Razzakov, Kyrgyz Republic, 720044 Mir Avenue 66, e-mail: dmitriy.matyushin@m-vector.com*

Abdyllaeva Gulnara Omorovna, *PhD, Associate professor, KSTU named after I.Razzakov, Kyrgyzstan, 720044, Bishkek, Kyrgyzstan,* e-mail: *g.abdyllaeva@mail.ru*

The purpose of this article: Issues consideration of the Data center information security and, including strict requirements for information security. And consideration of physical security by providing transparent access to customers via Internet.

Keywords: Data center, information security, Internet, information leakage.

Вероятность атаки на Центр обработки данных велика. Это связано с большим количеством размещаемой в нем информации, большая часть которой может быть критически важной для отдельно взятой организации. Для начала разберемся, что же представляет из себя Центр обработки данных.

Центр обработки данных (ЦОД) - это структура, ориентирующаяся на предоставление комплексных услуг, которые могут требоваться корпоративному заказчику. ЦОД характеризуется как высоко защищенная территория, с надежными техническими и организационными мерами безопасности, в которых имеется своя специфика.

К примеру, это соблюдение жестких требований к информационной безопасности при обеспечении прозрачного доступа клиентам через сеть Интернет.

Ещё одна особенность ЦОД это использование различных приложений и платформ, необходимых для клиентов, что приводит к осложнению возможности сконцентрироваться на защите какой-либо одной платформы или продукта.

Так же не стоит забывать, что часть информации может быть конфиденциальной, и доступ к ней не должен никто, кроме клиента.

Постоянную проблему представляет собой генерация и смена паролей суперпользователей. Пароль - совокупность символов, известных подключенному к сети абоненту, - вводится им в начале сеанса взаимодействия с сетью, а иногда и в конце сеанса (в особо ответственных случаях пароль нормального выхода из сети может отличаться от входного). Эта схема является наиболее уязвимой с точки зрения безопасности - пароль может быть перехвачен и использован другим лицом. Чаще всего используются схемы с применением одноразовых паролей. Даже будучи перехваченным, этот пароль будет бесполезен при следующей регистрации, а получить следующий пароль из предыдущего является крайне трудной задачей. Для генерации одноразовых паролей используются как программные, так и аппаратные генераторы, представляющие собой устройства, вставляемые в слот компьютера. Да, конечно, из соображений безопасности пароли действительно следует менять часто. Но, к сожалению, пользователи, которые часто меняют пароли, хранят эту информацию на рабочем столе компьютера в файле с названием «Пароль», а это не есть хорошо, в плане безопасности. Неплохим выходом из этой ситуации может стать применение современных средств идентификации и контроля доступа на основе смарт-карт, а также системы биометрического контроля.

Системы биометрического контроля являются предпочтительнее, так как карту можно потерять или забыть дома, в то время как пальцы или глаз потерять, или забыть сложнее.

Защиту ЦОД можно условно поделить на несколько рубежей «обороны»:

- сокрытие структуры сети, или имитационная защита. Эмуляция сети: сегменты, серверы, уязвимости. Контролируя атаки на эту «ложную» сеть можно выявить источники угроз. Так же такая сеть вводит в заблуждение потенциальных злоумышленников и усложняет задачу взлома сети и планирования атаки.

- детекторы вторжений, IDS. Данная система анализирует весь входящий траффик, отслеживая при этом известные типы атак. При этом в некоторых случаях используется система адаптивной защиты, которая изменяет списки доступа на межсетевом экране.

- разделение зон безопасности, закрытых сетевыми экранами, и разделение трафика за счет виртуальных сетей VPN. Трехуровневая структура (внешняя зона, демилитаризованная зона и внутренняя зона) является стандартным решением.

- контроль доступа и идентификация пользователей. Тут стоит остановиться на контроле доступа администраторов и операторов, имеющих административные полномочия в системе.

Еще один немаловажный момент – корпоративная политика и этика. Так как в ЦОД работает большое количество людей, которые в том числе отвечают и за безопасность, нужно стимулировать лояльность сотрудников. Если сотрудник лоялен организации, он вряд ли станет инсайдером и не будет сливать различного рода информацию третьим лицам или конкурентам. Таким образом вероятность утечки информации будет сведена к минимуму.

Физическая защита ЦОД

Итак, в нашем гипотетическом ЦОД развитая защита информации. Но что же обстоит с физической защитой? Ее нельзя недооценивать, потому как сотрудники, случайно оказавшиеся в машинном отделение могут организовать огромное количество проблем, которые в свою очередь приведут к финансовым потерям. Однако степени защиты (замки на дверях и т.д.) подразделяются на несколько уровней. И какой уровень выбрать зависит о целей отдельно взятого ЦОД. В таблице №1 ниже представлены некоторые необходимые меры физической безопасности в зависимости от категории ЦОД.

Таблица 1. Некоторые необходимые меры физической безопасности в зависимости от категории ЦОД.

Пуленепробиваемые стены, окна и двери:	**Tier I**	**Tier II**	**Tier III**	**Tier IV**
• Пропускной пункт в лобби	н/п	н/п	Уровень 3 min	Уровень 3 min
• Пропускной пункт в зоне разгрузки/погрузки	н/п	н/п	н/п	Уровень 3 min
Видеонаблюдение:	**Tier I**	**Tier II**	**Tier III**	**Tier IV**
• Периметр здания и паркинг	Нет требований	Нет требований	Да	Да
• Генераторы	н/п	н/п	Да	Да
• Контролируемые входы	Нет требований	Да	Да	Да
• Этажи с машзалами	Нет требований	Да	Да	Да
Контроль доступа/ мониторинг безопасности для:	**Tier I**	**Tier II**	**Tier III**	**Tier IV**
• Запасные выходы	Профессиональные замки	Мониторинг	Выход по коду	Выход по коду
• Наружные окна	Наружный мониторинг	Контроль проникновения	Контроль проникновения	Контроль проникновения
• Центр управления безопасностью	н/п	н/п	Доступ по карточкам	Доступ по карточкам
• Двери в машзал	Профессиональные замки	Контроль проникновения	Доступ по карточкам / биометрический контроль входа и выхода	Доступ по карточкам / биометрический контроль входа и выхода
• Колодцы с оптическим кабелем	Профессиональные замки	Контроль проникновения	Контроль проникновения	Доступ по карточкам

Наиболее сбалансированный способ обеспечить физическую безопасность ЦОД это возможность реализовать многоуровневую защиту (с несколькими периметрами безопасности). Как и при эшелонированной обороне, прорыв одного уровня не будет означать прорыва системы безопасности. При этом внутренние периметры безопасности не менее важны, чем внешние: они позволяют уменьшить риск реализации внутренних угроз вследствие как непреднамеренных, так и злонамеренных действий сотрудников.

Согласно опросу Cyber-ark, из 600 финансовых работников, отвечавших на вопросы в Нью-Йорке и Лондоне, 25% респондентов признали, что они не преминут воспользоваться служебной информацией в собственных целях, несмотря на любые последствия, при этом большинство осознает незаконность своих действий. Так что опасения работодателей (69% из них видят наибольшую угрозу безопасности в действиях собственного персонала) выглядят вполне обоснованными.

Если необходимость организации контроля доступа осознают все владельцы центров обработки данных, то разграничением доступа внутри ЦОД многие пренебрегают. Очень часто можно встретить следующую ситуацию: ЦОД имеет охраняемый периметр, доступ на объект строго ограничен, но вот проход в машинный зал открыт для всего обслуживающего персонала, и любой сотрудник, сам не зная того, может создать опасную ситуацию, которая приведет к остановке ЦОД. И ведь это не пустые предостережения. Валентин Фосс, директор по маркетингу и продажам компании «Утилекс», рассказал в качестве примера поучительную историю. На одном из объектов внештатный электрик, приглашенный в ЦОД для проведения каких-то незначительных работ, был оставлен без присмотра. Из чистого любопытства он нажал на кнопку аварийного пожаротушения. В результате была повреждена часть оборудования, не говоря уж о внеплановой остановке работы всего ЦОД.

Таким образом, если обслуживающий персонал (а в случае коммерческого ЦОД и сами клиенты) будет иметь свободный доступ в машинный зал, то вероятность нанесения вреда данным очень высока, даже несмотря на наличие многоуровневой системы безопасности. Избежать этого поможет только продуманная политика ограничения доступа. При этом система доступа должна служить инструментом для реализации этой политики. В противном случае вся многоуровневая система безопасности теряет смысл. Между тем, как указывает Валентин Фосс, при разработке комплексов физической защиты ЦОД зачастую не уделяется должного внимания сквозному процессу подготовки персонала и управления им, для чего нужны должностные инструкции, разграничение прав доступа и многое другое. Пренебрежение любой из составляющих может привести к неожиданным и крайне негативным последствиям.

Количество периметров безопасности зависит от требований, предъявляемых к площадке, с учетом оценки вероятности реализации угроз, приемлемого варианта обработки рисков и принятой политики безопасности. Определить, сколько уровней контроля доступа должно быть, можно только при условии рассмотрения совокупности факторов, таких как место расположения и степень важности ЦОД, риски по факторам вандализма (преднамеренного и случайного) и несанкционированного доступа. Идеальной считается система с четырьмя уровнями контроля доступа — на внешнем периметре, при входе в здание, в машинный зал и на уровне стойки. На практике чаще всего встречается двухуровневая система (здание/зал). Достаточным является частичное ограничение доступа по трем уровням (здание/зал/стойка). Однако некоторые специалисты выделяют иные три уровня: периметр (входы, въезды, прилегающая территория); буферные зоны с пропускным пунктом при входе в здание, охраняемый въезд в разгрузочную зону; залы и инженерные помещения (как пример). Для некоторых коммерческих ЦОД может потребоваться еще один: ограждение стоек.

В случае же высоких требований к безопасности уровней может быть гораздо больше. Так, Фред Дикермэн, вице-президент, начальник эксплуатации ЦОД DataSpace1, выделяет по меньшей мере пять зон: внешний периметр, внутренний периметр, вход в здание (свободный доступ в приемную, но закрытый доступ во внутреннее лобби), места размещения критического инфраструктурного оборудования, комнаты службы безопасности (пункт охраны, студия мониторинга). Помимо этого, коммерческим ЦОД могут понадобиться еще три зоны — для машинных залов, пространств внутри залов и отдельных стоек. Таким образом, всего придется создать 8 зон. Все эти деления достаточно условны и в общем случае могут быть сведены к четырем типовым (см. Рисунок 1) путем объединения в группы

дополнительных зон безопасности. К тому же физическая безопасность ЦОД — это не только и не столько определенное количество периметров защиты, сколько продуманная стратегия защиты данных в соответствии с конкретной моделью угроз

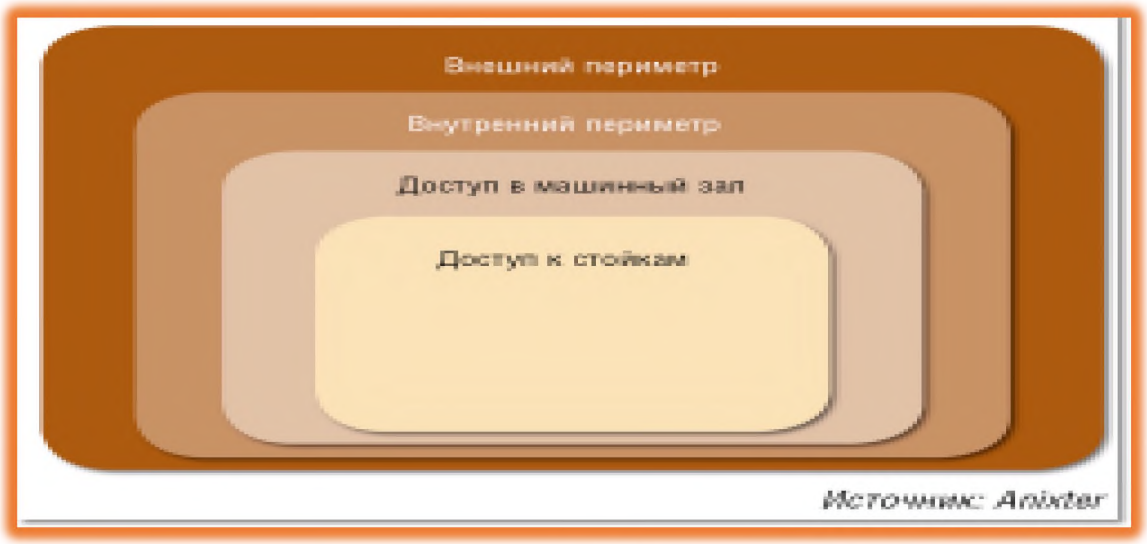

Рис. 1.
Четыре уровня физической безопасности ЦОД.

В заключение можно сказать, что ЦОД это сложный «механизм», который проблематично и дорого защищать, потому как причиной взлома может стать и сотрудник, случайно (или преднамеренно) оказавшийся в машинном отделении. Поэтому помимо защиты с точки зрения информационной безопасности, необходимо задуматься и о качественной физической защите, в том числе и о разграничении доступа в различные части ЦОД.

Как было описано выше, применимые меры полностью зависят от назначения ЦОД. Чем выше его важность, тем выше должны быть меры безопасности. К примеру обычные замки желательно заменить на, хотя-бы замки с пропуском по ID-картам. Так же немаловажной будет лояльность сотрудников. Защита ЦОД с точки зрения информационной безопасности поможет защититься от внешних угроз, тогда как физическая защита поможет снизить вероятность вреда как от штатных сотрудников, так и злоумышленников, проникших в здание.

Список литературы

1. .Д.Векслер (Дж. Векслер) Наконец-то надежно обеспечена защита данных в радиосетях // Компьютеруорлд Москва, 1994, N17, сс. 13-2. Регис Дж. Бейтс Физическая защита // в аварийном восстановлении для ЛВС, 1994, McGraw-Hill, Inc, pp. 44-б5

2. М. Рааб (M.Raab) Защита сетей: наконец-то в центре внимания // Компьютеруорлд Москва, 1994, №29, с. 18

3. Безопасность компьютерных коммуникаций Warwick Ford. Принципы, стандартные протоколы и методы // PTR Prentice Hall, 1994, 500р.

4. Проблемы финансов / банковской безопасности: обзор за 1994 год // Доклады Datapro по автоматизации банковской деятельности McGraw-Hill Inc., февраль 1995 г., стр. 101-108

5. Датапро на CD-ROM Communications Analyst, 1994, октябрь.

6. С.В. Сухова. Система безопасности NetWare // "Cemu", 1995, N4, сс. 60-70