Бердник Алексей Вячеславович

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ. АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОБЛАКОВ ОТ CLOUD SECURITY ALLIANCE

В статье рассматриваются различные виды существующих угроз облачных вычислений (англ. Cloud Computing). Анализируются атаки на элементы облака и решения по их устранению, а также апробация решения по защите от угроз безопасности облаков от компании Cloud Security Alliance (CSA). Предложены решения по защите от угроз безопасности облачных вычислений.

Адрес статьи: www.gramota.net/materials/1/2013/10/9.html
Статья опубликована в авторской редакции и отражает точку зрения автора(ов) по рассматриваемому вопросу.

Источник
Альманах современной науки и образования
Тамбов: Грамота, 2013. № 10 (77). С. 35-38. ISSN 1993-5552.
Адрес журнала: www.gramota.net/editions/1.html
Содержание данного номера журнала: www.gramota.net/materials/1/2013/10/

является подзаконным актом, принятым во исполнение закона» [3, с. 15]. Однако указанная позиция, на наш взгляд, не совсем применима в отношении акта об объявлении налоговой амнистии.

Если правоприменительный акт имеет разовое применение и индивидуальный характер, нельзя то же самое сказать в отношении акта об объявлении налоговой амнистии, поскольку он принимается и действует в определенный период времени, но рассчитан на многократное применение в период его действия и направлен не в отношении индивидуального лица, а в отношении неопределенного круга лиц конкретной категории налогоплательщиков.

Однако во исполнение акта об объявлении налоговой амнистии, принятого законодательным органом Российской Федерации, на основании заявлений налогоплательщиков налоговым органом принимается акт о списании недоимок лица, который, в свою очередь, уже нельзя рассматривать как нормативно-правовой. В таком случае его следует признать правоприменительным актом, поскольку указанное решение принимается во исполнение действующих норм об объявлении налоговой амнистии и в отношении индивидуального лица.

Изложенное свидетельствует, что акт об объявлении налоговой амнистии носит двойственный характер и в зависимости от органа, принимающего акт об объявлении налоговой амнистии, может являться либо нормативно-правовым, либо правоприменительным. В целях устранения неясностей в характере акта налоговой амнистии необходимо реформирование действующего законодательства, в частности налогового, – внести в главу 15 Налогового кодекса РФ статью, регламентирующую порядок объявления налоговой амнистии Государственной Думой Федерального Собрания Российской Федерации в виде постановления.

Список литературы

1. **Алексеев С. С.** Теория государства и права: учебник для вузов. М., 2001.
2. **Конституция Российской Федерации** (принята всенародным голосованием 12.12.1993) // Российская газета. 2009. 21 января.
3. **Марогулова И. Л.** Законодательное регулирование амнистии и помилования: автореф. дисс. … д.ю.н. М., 1999.
4. **О проведении налоговой амнистии в 1993 году** [Электронный ресурс]: Указ Президента РФ от 27.10.1993 № 1773. Доступ из СПС «КонсультантПлюс».
5. **Об упрощенном порядке декларирования доходов физическими лицами**: Федеральный закон от 30.12.2006 № 269-ФЗ // Российская газета. 2006. 31 декабря.
6. **Теория государства и права**: курс лекций / под ред. Н. И. Матузова и А. В. Малько. 2-е изд., перераб. и доп. М.: Юристъ, 2001. 776 с.

ACT OF TAX AMNESTY AS ITS EXPRESSION FORM: CHARACTERISTIC FEATURES AND PECULIARITIES

Belova Tat'yana Aleksandrovna
Saratov State Academy of Law
t_a_belova88@mail.ru

The article is devoted to studying the question on the kind of the act of tax amnesty as one of legal acts. Using the methods of comparison and correlation the characteristic features of the act of tax amnesty as simultaneously a normative-legal and law-enforcement act are revealed. Basing on the conducted analysis, the author for the first time suggests including the norms regulating the order of tax amnesty pronouncement into the Tax Code of the Russian Federation.

Key words and phrases: humanism principle; tax amnesty; law; form of law; normative act; normative-legal act; interpretative act; law-enforcement act.

УДК 004.457
Технические науки

В статье рассматриваются различные виды существующих угроз облачных вычислений (англ. Cloud Computing). Анализируются атаки на элементы облака и решения по их устранению, а также апробация решения по защите от угроз безопасности облаков от компании Cloud Security Alliance (CSA). Предложены решения по защите от угроз безопасности облачных вычислений.

Ключевые слова и фразы: облачные вычисления; информационная безопасность; виртуальная среда; атаки на облака; *Cloud Security Alliance*.

Бердник Алексей Вячеславович
Тюменский государственный университет
avberdnik@gmail.com

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ. АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ОБЛАКОВ ОТ *CLOUD SECURITY ALLIANCE*©

Центр обработки данных (ЦОД) (англ. *Data Center*) представляет собой совокупность серверов, размещенных на одной площадке с целью повышения эффективности и защищенности. Защита центров обработки данных включает сетевую и физическую защиту, а также отказоустойчивость и надежное электропитание.

В настоящее время на рынке представлен широкий спектр решений для защиты серверов и ЦОД от различных угроз. Их объединяет ориентированность на узкий спектр решаемых задач [1]. Однако он подвергся некоторому расширению вследствие постепенного вытеснения классических аппаратных систем виртуальными платформами. К известным типам угроз (сетевые атаки, уязвимости в приложениях операционных систем, вредоносное программное обеспечение) добавились сложности, связанные с контролем среды (гипервизора), трафика между гостевыми машинами и разграничением прав доступа. Расширились внутренние вопросы и политики защиты ЦОД, требования внешних регуляторов. Работа современных ЦОД в ряде отраслей требует закрытия технических вопросов, а также вопросов, связанных с их безопасностью. Финансовые институты (банки, процессинговые центры) подчинены ряду стандартов, выполнение которых заложено на уровне технических решений. Проникновение платформ виртуализации достигло того уровня, когда практически все компании, использующие эти системы, весьма серьезно занялись вопросами усиления безопасности в них. Отметим, что буквально год назад интерес был скорее теоретический [3; 8]. В современных условиях становится все сложнее обеспечить защиту критически важных для бизнеса систем и приложений [1].

Появление виртуализации стало актуальной причиной масштабной миграции большинства систем на виртуальные машины (ВМ), однако решение задач обеспечения безопасности, связанных с эксплуатацией приложений в новой среде, требует особого подхода. Многие типы угроз достаточно изучены, и для них разработаны средства защиты, однако их еще нужно адаптировать для использования в облаке.

Существующие угрозы облачных вычислений

Контроль и управление облаками являются проблемой безопасности. Гарантий, что все ресурсы облака посчитаны, и в нем нет неконтролируемых виртуальных машин, не запущено лишних процессов, и не нарушена взаимная конфигурация элементов облака, нет. Это – высокоуровневый тип угроз, т.к. он связан с управляемостью облаком как единой информационной системой, и для него общую защиту нужно строить индивидуально. Для этого необходимо использовать модель управления рисками для облачных инфраструктур.

В основе обеспечения физической безопасности лежит строгий контроль физического доступа к серверам и сетевой инфраструктуре. В отличие от физической безопасности, сетевая безопасность в первую очередь представляет собой построение надежной модели угроз, включающей в себя защиту от вторжений и межсетевой экран. Использование межсетевого экрана подразумевает работу фильтра с целью разграничить внутренние сети ЦОД на подсети с разным уровнем доверия. Это могут быть отдельно серверы, доступные из Интернета, или серверы из внутренних сетей.

В облачных вычислениях важнейшую роль платформы выполняет технология виртуализации. Для сохранения целостности данных и обеспечения защиты рассмотрим основные известные угрозы для облачных вычислений.

1. Трудности при перемещении обычных серверов в вычислительное облако

Требования к безопасности облачных вычислений не отличаются от требований безопасности к центрам обработки данных. Однако виртуализация ЦОД и переход к облачным средам приводят к появлению новых угроз.

Доступ через Интернет к управлению вычислительной мощностью – одна из ключевых характеристик облачных вычислений. В большинстве традиционных ЦОД доступ инженеров к серверам контролируется на физическом уровне, в облачных средах они работают через Интернет. Разграничение контроля доступа и обеспечение прозрачности изменений на системном уровне являются одними из главных критериев защиты.

2. Динамичность виртуальных машин

Виртуальные машины динамичны. Они клонируются и могут быть перемещены между физическими серверами. Данная изменчивость влияет на разработку целостности системы безопасности. Однако уязвимости операционной системы или приложений в виртуальной среде распространяются бесконтрольно и часто проявляются после произвольного промежутка времени (например, при восстановлении из резервной копии). В среде облачных вычислений важно надежно зафиксировать состояние защиты системы, независимо от ее местоположения.

3. Уязвимости внутри виртуальной среды

Серверы облачных вычислений и локальные серверы используют одни и те же операционные системы и приложения. Для облачных систем угроза удаленного взлома или заражения вредоносным ПО высока. Риск для виртуальных систем также высок. Параллельные виртуальные машины увеличивает «атакуемую поверхность». Система обнаружения и предотвращения вторжений должна быть способна обнаруживать вредоносную активность на уровне виртуальных машин, вне зависимости от их расположения в облачной среде.

4. Защита бездействующих виртуальных машин

Когда виртуальная машина выключена, она подвергается опасности заражения. Доступа к хранилищу образов виртуальных машин через сеть достаточно. На выключенной виртуальной машине абсолютно невозможно запустить защитное программное обеспечение. В данном случае должна быть реализована защита не только внутри каждой виртуальной машины, но и на уровне гипервизора.

5. Защита периметра и разграничение сети

При использовании облачных вычислений периметр сети размывается или исчезает. Это приводит к тому, что защита менее защищенной части сети определяет общий уровень защищенности. Для разграничения сегментов с разными уровнями доверия в облаке виртуальные машины должны сами обеспечивать себя защитой, перемещая сетевой периметр к самой виртуальной машине (Рис. 1). Корпоративный *firewall* – основной компонент для внедрения политики IT-безопасности и разграничения сегментов сети – не в состоянии повлиять на серверы, размещенные в облачных средах [4].

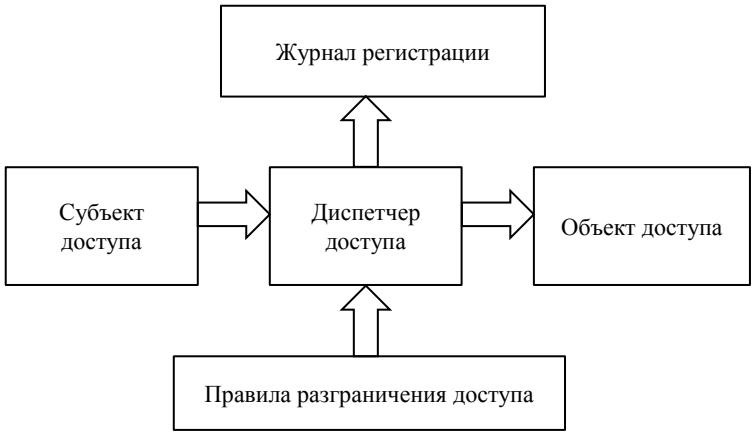

Рис. 1. *Схема работы механизма разграничения доступа* [7]

Атаки на облака и решения по их устранению

1. Традиционные атаки на ПО

Уязвимости операционных систем, модульных компонентов, сетевых протоколов – традиционные угрозы, для защиты от которых достаточно установить межсетевой экран, *firewall*, антивирус, систему предотвращения вторжений (Intrusion Prevention System – IPS) и другие компоненты. При этом важно, чтобы данные средства защиты эффективно работали в условиях виртуализации.

2. Функциональные атаки на элементы облака

Этот тип атак связан с многослойностью облака, общим принципом безопасности. В статье об опасности облаков было предложено следующее решение [4]: для защиты от функциональных атак для каждой части облака необходимо использовать следующие средства защиты: для прокси – эффективную защиту от DoS-атак, для веб-сервера – контроль целостности страниц, для сервера приложений – экран уровня приложений, для СУБД – защиту от SQL-инъекций, для системы хранения данных – правильные бэкапы (резервное копирование), разграничение доступа. В отдельности каждые из этих защитных механизмов уже созданы, но они не собраны вместе для комплексной защиты облака, поэтому задачу по интеграции их в единую систему нужно решать во время создания облака.

3. Атаки на клиента

Большинство пользователей подключаются к облаку, используя браузер. Здесь рассматриваются такие атаки как *Cross Site Scripting*, «угон» паролей, перехваты веб-сессий, «человек посредине» и многие другие. На текущий момент, наиболее эффективной защитой от данного вида атак является правильная аутентификация и использование шифрованного соединения (SSL) с взаимной аутентификацией [5]. Однако данные средства защиты не очень удобны и очень расточительны для создателей облаков. В этой отрасли информационной безопасности есть еще множество нерешенных задач.

4. Атаки на гипервизор

Гипервизор является одним из ключевых элементов виртуальной системы. Основной его функцией является разделение ресурсов между виртуальными машинами. Атака на гипервизор может привести к тому, что одна виртуальная машина сможет получить доступ к памяти и ресурсам другой. Также она сможет перехватывать сетевой трафик, отбирать физические ресурсы и даже вытеснить виртуальную машину с сервера. В качестве стандартных методов защиты рекомендуется применять специализированные продукты для виртуальных сред, интеграцию хост-серверов со службой каталога *Active Directory*, использование политик сложности и устаревания паролей, а также стандартизацию процедур доступа к управляющим средствам хост-сервера, встроенный брандмауэр хоста виртуализации. Также возможно отключение таких часто неиспользуемых служб как, например, веб-доступ к серверу виртуализации.

5. Атаки на системы управления

Большое количество виртуальных машин, используемых в облаках, требует наличия систем управления, способных надежно контролировать создание, перенос и утилизацию виртуальных машин. Вмешательство в систему управления может привести к появлению виртуальных машин – невидимок, способных блокировать одни виртуальные машины и подставлять другие.

Решения по защите от угроз безопасности от компании *Cloud Security Alliance* (CSA)

Наиболее эффективные способы защиты в области безопасности облаков опубликовала организация *Cloud Security Alliance* (CSA). Проанализировав опубликованную компанией информацию, были предложены следующие решения [6]:

1. Сохранность данных. Шифрование

Шифрование – один из самых эффективных способов защиты данных. Провайдер, предоставляющий доступ к данным, должен шифровать информацию клиента, хранящуюся в ЦОД, а также, в случае отсутствия необходимости, безвозвратно удалять.

2. Защита данных при передаче

Зашифрованные данные при передаче должны быть доступны только после аутентификации. Данные не получится прочитать или сделать изменения, даже в случае доступа через ненадежные узлы. Такие технологии достаточно известны, алгоритмы и надежные протоколы AES, TLS, IPsec давно используются провайдерами.

3. Аутентификация

Аутентификация – защита паролем. Для обеспечения более высокой надежности часто прибегают к таким средствам как токены и сертификаты. Для прозрачного взаимодействия провайдера с системой идентификации при авторизации также рекомендуется использовать LDAP (Lightweight Directory Access Protocol) и SAML (Security Assertion Markup Language).

4. Изоляция пользователей

Использование индивидуальной виртуальной машины и виртуальной сети. Виртуальные сети должны быть развернуты с применением таких технологий как VPN (Virtual Private Network), VLAN (Virtual Local Area Network) и VPLS (Virtual Private LAN Service). Часто провайдеры изолируют информацию пользователей друг от друга за счет изменения кода в единой программной среде. Такой подход имеет риски, связанные с опасностью найти «дыру» в нестандартном коде и получить доступ к данным пользователей. В случае возможной ошибки в коде один пользователь может получить данные другого пользователя.

Заключение

Описанные решения по защите от угроз безопасности облачных вычислений неоднократно были применены системными интеграторами в проектах построения частных облаков. Практические применения и требования по безопасности подробно описаны в тезисах [1; 2]. После применения данных решений количество случившихся инцидентов существенно снизилось. Но многие проблемы, связанные с защитой виртуализации, до сих пор требуют тщательного анализа и проработанного решения.

Список литературы

1. **Бердник А. В.** Сравнительный анализ решений по безопасности SaaS сервиса от компании IBM и КРОК // Безопасность информационного пространства: сборник статей. Тюмень, 2012. С. 245-253.
2. **Бердник А. В., Бойко А.** Методы защиты виртуальной среды // Всероссийский журнал научных публикаций. 2013. № 3 (18). С. 24-27.
3. **Емельянова Ю. Г., Фраленко В. П.** Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления [Электронный ресурс] // Программные системы: теория и приложения. 2011. № 4 (8). С. 17-31. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf (дата обращения: 19.08.2013).
4. **Коржов В.** Опасны ли облака? [Электронный ресурс] // Сети / Network World. 2010. № 07. URL: http://www.osp.ru/nets/2010/07/13004633/ (дата обращения: 19.08.2013).
5. **Облака: легенды и мифы** [Электронный ресурс]. URL: http://www.anti-malware.ru/node/2333 (дата обращения: 19.08.2013).
6. **Облачные вычисления, «дырявые» облака и способы защиты данных** [Электронный ресурс]. URL: http://4by4.ru/ru/analytics/oblachnye-vychisleniya-dyryavye-oblaka-i-sposoby-zashchity-dannyh (дата обращения: 19.08.2013).
7. **Основные защитные механизмы, используемые в СЗИ** [Электронный ресурс]. URL: http://asher.ru/security/book/its/07 (дата обращения: 19.08.2013).
8. **Романов Н.** Реальные проблемы виртуальных ЦОД [Электронный ресурс] // Jet Info. 2012. № 3. URL: http://www.jetinfo.ru/jetinfo_arhiv/zaschita-virtualnykh-sred/realnye-problemy-virtualnykh-tsod/2012 (дата обращения: 19.08.2013).

CLOUD COMPUTING SECURITY PROBLEMS. ANALYSIS OF CLOUDS PROTECTION METHODS SUGGESTED BY *CLOUD SECURITY ALLIANCE*

Berdnik Aleksei Vyacheslavovich
Tyumen State University
avberdnik@gmail.com

Different types of existing cloud computing threats are considered in the article. Cloud elements attacks and their eliminati on solutions as well as the approbation of the solution concerning the protection from clouds security threats suggested by the company *Cloud Security Alliance* (CSA) are analyzed. Solutions concerning the protection from cloud computing security threats are presented.

Key words and phrases: cloud computing; information security; virtual environment; clouds attacks; *Cloud Security Alliance*.