УДК 004.056.5:004.052:004.41

УЯЗВИМОСТИ КОНВЕРГЕНТНОЙ ИНФРАСТРУКТУРЫ И ПРАКТИЧЕСКИЕ ПОДХОДЫ К ИХ УСТРАНЕНИЮ

Зеленцова Ж.Ю., Луговой А.В.

CRITICAL CONVERGED INFRASTRUCTURE VULNERABILITY AND PRACTICAL APPROACHES TO THEIR ELIMINATION

Lugovoi A., Zelentsova Zh.

Проведен агрегированный анализ угроз в конвергентной инфраструктуре с целью создания защищенных прикладных конвергентных систем мониторинга для IoT-устройств. Практические подходы по обеспечению безопасности рассмотрены на модели развертывания.

Ключевые слова: *уязвимости конвергентной инфраструктуры, методы защиты облаков*

Актуальность и задача исследования. С течением времени изменяются архитектурные подходы в организации вычислительных сетей и систем, в настоящий момент характеризующихся высоким уровнем сложности и многообразием. В их рамках рассматриваются системы ИТ-безопасности, прежде всего, направленные на защиту конфиденциальных данных в полностью или частично открытых средах. При этом согласно прогнозам [1,2,3] определяются три крупные проблемы, которые будут свойственны глобальной сети в ближайшей перспективе – *проблема большого количества данных*, *проблема большого количества устройств* и *проблема большого количества пользователей*. Они могут быть рассмотрены в совокупности и отдельно. Эти проблемы будут, соответственно, требовать выработки новых подходов организации сети и выдвигать новые требования к безопасности.

Ожидаемые изменения вычислительной архитектуры, а именно, появление архитектуры V поколения для сетевой и открытой инфраструктуры, уже на сегодняшний день требуют принципиально новых «архитектурных» способов обеспечения безопасности с целью решения перечисленных проблем. В данном исследовании рассматриваются архитектурные уязвимости и практические подходы к их устранению с выработкой модели инфраструктуры, ориентированной на системы безопасности, обслуживающие устройства, в целях многофакторного, мультиобъектного и многоцелевого мониторинга. Решение может быть масштабировано на аналогичные гетерогенные среды, в которых требуется безопасное и эффективное управление большим количеством устройств и данными, ими формируемыми.

Материал и результаты исследования. Согласно прогнозу IDC [1], объем сетевых данных с 2011 по 2020 год увеличится с 1,8 до 35 зеттабайт (до 35 млрд. террабайт) – на сегодняшний день уже наблюдается слабая структурируемость и незащищенность данных в сети. Данные формируются пользователями посредством персональных устройств, а также устройствами, обеспечивающими своей функциональностью промышленные, гражданские и военные процессы.

По прогнозу Cisco [2,3,4,5], количество мобильных устройств к 2015 году будет в два раза превышать прогнозируемое население Земли, это составит 19 млрд. сетевых устройств в 2017 году по сравнению с 12 млрд. в 2012 году, а количество интернет-пользователей достигнет 40% от прогнозируемого населения, по уточненным данным это составит 3,6 млрд. человек в 2017 году по сравнению с 2,3 млрд. в 2012 году, сервисами мобильной коммерции в 2017 году будет пользоваться 2,6 млрд. пользователей, против 560 млн. в 2012 году. По прогнозу Cisco [2,3], до 2015 года возрастет трафик от телевизоров, устройств M2M, Smart Grid (non-PC): от ПК – на 33%, от телевизоров – на 101%, от смартфонов – на 144%, от устройств M2M – на 258 %.

В ближайшей перспективе потребуется обеспечение безопасности передаваемых от устройств данных, как находящихся в хранилищах, так при их передаче по магистральным сетям. Проблема безопасности данных тесно связана с проблемой больших данных: по прогнозам к 2015 году общий сетевой трафик будет равен 7,3 петабайт каждые 5 минут, а 50% трафика составят видеофайлы, а сеть будет иметь мультимедийный характер [2,3].

Таким образом, очевидна необходимость разработки систем управления устройствами и данными ими генерируемыми. Технологический класс развиваемых программно-аппаратных решений IoT (Internet of Things) в будущем объединит целый ряд инструментов для управления устройствами, подключенными к сети – это могут быть машины, датчики, автомобили и «интернет-вещи», которые помогут улучшить пользователям качество жизни. Портфель приложений для сетевых устройств IoT дополнится приложениями типа «Интернет для всего» или Internet of Everything (IoE),

расширяющими функциональные возможности IoT [6]. Semico Research опубликовало результаты доклада о следующей волне приложений IoT, это: системы управления устройствами ЖКХ, электроучета и энергообеспечения; удаленный мониторинг домов и бытовой техники; системы безопасности, мониторинга, видеонаблюдения частного и промышленного характера; системы управления запасами в бизнесе и торговле, удаленный доступ к развлечениям [7].

Цифры прогнозов однозначно определяют, что интенсивный рост количества устройств типа IoT и пользователей продолжится, функциональность будет расширяться, при этом задействованные объемы информации потребуют использования высокопроизводительных ресурсов для их обработки.

Пользователи, системы учета, сетевые бытовые приборы, различные аппаратные системы прямого или косвенного слежения кроме обычных формируют множество промежуточных данных – *цифровой след* и *цифровую тень* – они могут быть связаны с определенным объектом или пользователем [1]. Цифровой след формируется при активных действиях пользователей, цифровая тень создается устройствами и системами о пользователях.

Большая часть этих данных, включая системы общего назначения, относятся к конфиденциальным, соответственно, должен быть обеспечен требуемый уровень защиты [1]. Отдельную нишу занимают системы специального назначения, которые также относятся к приложениям типов IoT и IoE, так как современные технологии позволяют автоматизировать процессы мониторинга систем энергоснабжения, коммунальных сетей, безопасности, включая системы городского видеонаблюдения за общественными местами, охраны границ, промышленных объектов и других.

Объем генерируемых устройствами данных требует использования высокопроизводительных ресурсов, которые могут быть предоставлены в рамках новой сетевой парадигмы – *конвергентной инфраструктуры*. Конвергентное решение обеспечивает гибкий и хорошо управляемый доступ ко всем ресурсам своей подсети, основанный на технологиях виртуализации, что, в свою очередь, оборачивается проблемами обеспечения безопасности, тогда как критически-важные приложения потребуют высокого уровня защиты. На сегодняшний день это не представляется возможным из-за существующих архитектурных особенностей открытых сетевых систем и применяемых технологических решений. Тем не менее, проблема обеспечения требуемого уровня безопасности при управлении устройствами типа IoT в средах виртуализации, которые могут обеспечить обработку больших объемов данных, должна быть решена, а предложенное решение должно быть технологически реализуемо и развиваемо.

Исследование уязвимостей конвергентных решений. К широко известному факту относится заявление Джошуа Кормана (англ. Joshua Corman), на тот момент эксперта IBM, на конференции «Interop Las Vegas 2009», что виртуализация в имеющемся формате не готова к использованию в критически важных приложениях. Несмотря на многочисленные заверения крупнейших вендоров в защищенности конвергентных систем, на сегодняшний день среды виртуализации являются слабо защищенными.

Гибкость открытых систем, простота масштабирования, динамическая инфраструктура конвергентных систем оборачивается часто полностью неразрешимыми проблемами безопасности, несмотря на вполне приемлемые текущие результаты применения классических методов защиты, не рассчитанных на высокопрофессиональные внешние атаки, рассматриваемые в качестве угроз в системах IoT специального назначения.

Классические инструменты обеспечения безопасности в информационных системах подразумевают применение эффективных средств защиты: антивирусных приложений, сетевых экранов, спам-фильтров и др., но специфика архитектуры виртуальных сред требует совершенно иного подхода. Часто повышения надежности достигают за счет избыточности – при этом избыточный код предполагает экспоненциальный рост количества уязвимостей. В современных приложениях безопасность и производительность становятся компромиссами.

Выделим основные категории архитектурных уязвимостей конвергентной инфраструктуры, доступных для эксплойтов:

1. *Уязвимости, связанные со средствами виртуализации*, по данным IBM XForce на 2012 год насчитывалось 553 уязвимости средств виртуализации [8]:
   a) используемые виртуальные машины, посредством которых осуществляется доступ пользователей к высокопроизводительным ресурсам, и гипервизоры (микроОС) не имеют шифрования, что предполагает возможность атак при миграции виртуальных машин типа «man-in-the-middle» («человек посередине»). Атаки, связанные с нарушением работы гипервизора, составляют 38% [8].
   b) Виртуальные машины (VM) подвержены кражам, могут быть запущены нелегальные VM. После получения доступа к внутренней инфраструктуре это дает возможность

развернуть вредоносные приложения и осуществлять эффективные внутренние атаки с минимальными ограничениями по безопасности. Атаки, направленные на нарушение целостности VM составляют 35% [8].

c) Виртуализация дает возможность создания совершенных инструментов для проведения атак типа «man-in-the-middle». Примером вредоносной аппаратной виртуализации являются руткиты Blue Pill, реализуемые как устанавливаемые «на лету» гипервизоры. По утверждению разработчиков руткиты Blue Pill не могут быть обнаружены, существует возможность обнаружения применения технологий виртуализации, что не эффективно в средах виртуализации. Среди злоумышленников также популярны атаки на эмуляторы устройств. Внедрение кода в гостевую ОС составляет 15% от общего объема атак [8].

2. *Динамические уязвимости*, связанные со сложностью систем и избыточностью кода. Гипервизоры являются практически полноценными операционными системами, имеющими ошибки, предполагающие уязвимости. Устранение избыточного кода из VM нельзя считать достаточным условием эффективной защиты, так как всегда остается вероятность проведения атаки типа «Day-Zero» эксплойтом, использующим вновь обнаруженную уязвимость, методы защиты которой еще не разработаны.
3. *Уязвимости протокольного характера.* Этот класс уязвимостей связан с особенностями протокола TCP/IP – его неанонимным характером. Организация доступа по TCP/IP предполагает возможность установления доступа практически к любому устройству, подключенному к сети, и передачу управления злоумышленнику. К наиболее выраженным угрозам можно отнести атаки «man-in-the-middle» с целью паразитного мониторинга на атакуемых IoT мощностях, например, для проведения слежения за объектом с использованием атакуемой системы видеонаблюдения, а также с целью внесения искажений в обмен данных. Подобную возможность по обнаружению IoT устройств уже на сегодняшний день предоставляют API-сервисы поискового сервиса Shodan (www.shodanhq.com), разработанного компанией Google, в совокупности с руткитами Blue Pill;
4. *Уязвимости для паразитного использования процессоров* атакуемого объекта. Современные процессоры имеют несколько ядер, при этом чаще используются однопоточные приложения. Уязвимости, связанные с доступностью свободных ядер процессора при проектировании уровня «software» приложений, в совокупности с другими типами атак позволяют осуществлять скрытые вторжения и паразитный мониторинг не только для получения оперативной информации, но и для ее обработки на свободных ядрах процессоров атакуемой системы. Это возможно путем методом передачи пакета VMBus на vmswitch.sys. Для многоядерных и многопроцессорных систем может быть использован метод низкоуровневой защиты и обнаружения аппаратной виртуализации ядер процессоров Red Pill, разработанный специально для обнаружения руткитов Blue Pill в многопроцессорных системах.
5. *Унаследованные уязвимости распределенных систем.* Экземпляры операционных систем и приложения подвержены классическим атакам. Для данного класса разработаны эффективные методы защиты, такие как: аутентификация, метод открытых ключей и сертификациz, шифрование сетей и файловой системы,
6. *Унаследованные уязвимости пиринговых сетей.* Эта категория уязвимостей детально раскрывает проблемы безопасности распределенных систем и связана с хранением и передачей данный в пиринговых сетях типа P2P («peer-to-peer», «равный к равному»), которые положены в основу технологии вычислительной ткани – базовой компоненты конвергентной инфраструктуры, стандарта M2M («machine-to-machine») и беспроводных сенсорных сетей типа Smart Grid и др.

Архитектура конвергентной инфраструктуры предоставляет расширенные возможности для проведения внутренних и внешних атак. Платформа виртуализации состоит из множества компонентов - DHCP-сервер, NAT Device и др., которые становятся объектом вторжения. Тем не менее, согласно результатам исследования IBM XForce [8], меньше подвергаются атакам ресурсы, использующие IPv6. Также 50% конфиденциальной информации получается посредством социальных сетей. К одной из эффективных методик внедрения в виртуальную инфраструктуру является спам с вредоносными вложениями [8]. В 2012 году IBM публично раскрыла и обезвредила 8168 уязвимостей, несмотря на это утверждается, что

эффективные атаки связаны с нарушением политик безопасности, которые в 46% случаев приходятся на США, в 8% - на Британию, в 3% - на Австралию. 50% всех уязвимостей связаны с вебсайтами [8]. В 2012 году появилось 3436 публичных эксплойтов, что составляет 43% от общего количества устраненных брешей [8]. В целом за 2011 было отслежено 1088 атак, когда в 2012 году было зафиксировано 1502 попытки вторжения в виртуальную инфраструктуру IBM [8].

Для IoT-систем наиболее актуальны методы защиты, которые противостоят скрытому паразитному использованию устройств в целях атакующего. Для разработки эксплойтов доступен целый ряд приложений в открытом коде. Ограничением для атак такого рода остается трудоемкость разработки вредоносного программного обеспечения, которая сравнима с выпуском полноценной операционной системы. Тем не менее, подобные средства могут быть включены и разработаны в рамках секретной программы шпионажа PRISM, разработанной Агентством национальной безопасности США. Затраты будут оправданы, если объектами атаки и паразитного мониторинга IoT-устройств являются правительственные системы.

Устранение уязвимостей. Наряду с описанными уязвимостями можно утверждать, что виртуализация – это технологическая концепция и набор инструментов, в рамках которых могут быть реализованы беспрецедентные решения по организации внутренней и внешней защиты для специального и общего назначения. Как было отмечено, среды виртуализации требуют иных принципов развертывания, прежде всего, средств динамической защиты, чтобы исключить все виды атак, включая «Day-Zero».

Защищенность виртуальных машин. Одним из базовых моментов обеспечения безопасности в конвергентной инфраструктуре является соответствие виртуальной машины уровню защищенности. Для этих целей разработан специальный набор критериев оценки защищенности Common Criteria (англ. Common Criteria for Information Technology Security Evaluation), ISO/IEC 15408. Common Criteria является управляемой схемой сертификации правительственных систем. Критерии определяют целый ряд функциональных требований, требований доверия и профилей защиты к сервисам безопасности. В настоящий момент определено 7 уровней защищенности систем. Evaluation Assurance Level (EAL) описывает численный рейтинг глубины и строгости оценки.

Для примера облачное решение VMware vSphere 5.1 и VMware vCloud Networking, приобретенные компанией «Ростелеком» для нужд Правительства России, сертифицировано по EAL2+, что для облачных решений соответствует EAL4+. VMware vFabric (вычислительна ткань серверов) сертифицирована по EAL2+ [9].

При этом данную сертификацию, несмотря на высший уровень из доступных, нельзя считать условием достаточной безопасности в виртуальных средах. Методика сертификации предполагает самоопределение производителем модели окружения, злоумышленника и вторжения. Эти «предположения» ложатся в основу системы соответствия сертифицируемой системы заявленным параметрам. После прохождения сертификации могут быть обнаружены новые уязвимости, что потребует повторной сертификации, в противном случае сертификат отзывается.

Как отмечалось, архитектурная особенность динамических сред в наличии динамических уязвимостей. Статический подход обеспечения безопасности совершенно недопустим в динамических средах. Именно поэтому для облачных систем затруднена сертификация выше EAL2+ и EAL4+. Виртуальная машина XenSource от Citrix соответствует уровню EAL5+ [10]. В то же время, создать неуязвимую и защищенную виртуальную машину на сегодняшний день не представляется возможным, это связано с априорным наличием ошибок во всех без исключения программных приложениях.

Средства динамической защиты для систем общего назначения. Учитывая вышесказанное, рассматриваются способы включения систем безопасности, адаптивных к внутренним и внешним условиям, в защищенную инфраструктуру. Во многих конвергентных решениях реализованы отдельные сервера, которые отслеживают предполагаемые виды угроз и атак. В то же время по-настоящему специализированые решения для обеспечения безопасности виртуализации и облаков практически отсутствуют. Особенно критично выглядит эта проблема в IoT-системах специального назначения.

Сегодня наиболее востребована Akamai Intelligent Platform, предназначенная для облачных и клиент-серверных сред [11]. Платформой защиты в качестве угроз рассматриваются распространенные, интеллектуальные и эффективные атаки и решаются задачи: определение и блокирование угроз; мгновенная оптимизация уровня угроз; принятие решений на основе веб-условий. Платформа формирует адаптивную метамодель управления угрозами, динамическую модель поведения злоумышленника и состояния внешней среды – на основании пересечения требований принимаются решения смарт-системой. Akamai также предлагает платформу визуализации сетевого трафика и акселератор для повышения

надежности и скорости соединений Steelhead Cloud Accelerator, совместно разработанный с Riverbed Technology [12]. Это облачное приложение типа SaaS объединяет возможности Akamai Intelligent Platform и знаменитого решения Riverbed для оптимизации WAN-сетей и устраняет проблемы с безопасностью и производительностью, избежав компромисса. Это решение позволяет уменьшить объем трафика по транзитным соединениям и не расширять пропускную способность сети.

Имеется опыт использования Steelhead Cloud Accelerator для управления энергетическими IoT-сетями Schneider Electric – глобальной компании, специализирующейся на управлении энергетическими объектами [13]. К ресурсам Schneider Electric (www.schneider-electric.com) подключено более 16 тыс. пользователей, часть информации из LAN-сетей попадает в интернет (WAN-сети) и маршрутизируется по магистральным сетям (Tier-1), что приводит к росту задержек и росту рисков безопасности.

Создание проприетарных средств динамической защиты IoT сетей специального назначения. Очевидно, что безопасность, производительность и надежность соединение должны рассматриваться в совокупности и с учетом динамических параметров. Этот подход и реализован на базе Steelhead Cloud Accelerator. Несмотря на развитость решения Akamai по сравнению с другими предложениями, они не учитывают всех видов угроз, в IoT-сетях и свойственных конвергентной инфраструктуре, но предлагают качественное и доступное решение для систем общего назначения.

Для систем специального назначения, развернутых в конвергентной инфраструктуре, требуется разработать более развитую систему динамической защиты. Рекомендуемая для разработки и включения в конвергентную или облачную систему адаптивная к внешним и внутренним условиям облачная платформа безопасности включает в себя весь набор классических средств в совокупности: создание динамической модели системы и модели поведения злоумышленника, систему оценки рисков, сканирование и применение средств топологического анализа уязвимостей. Дополнительно, по опыту Akamai, классический набор инструментов защиты должен быть дополнен сетевым акселератором, оптимизирующим маршрутизацию по магистральным и внутренним сетям, а также сервисами, ориентированными на защиту уязвимостей виртуализации.

К средствам разработки относится инструмент для создания и тестирования эксплойтов Metasploit Framework, API-инструменты поисковой системы Shodan для тестирования доступности IoT-устройств из сети, открытый код руткитов Blue Pill для сокрытия функциональности IoT-сети, код метода Red Pill для защиты от паразитного использования процессоров, открытый код виртуальных машин. В связи с появлением Shodan для IoT-систем актуальна анонимизация трафика и сокрытие информации о местоположении узлов. Эффективные инструменты анонимизации трафика предоставляет набор протоколов Tor, а также доступный код организации «луковой» маршрутизации.

Способы анонимизации и шифрования трафика. Для анонимизации и шифрования трафика может быть использован Tor (англ. The Onion Router) – это проект свободного программного обеспечения с открытым кодом, использующий для анонимизации трафика, защищенную от прослушивания «луковую» маршрутизацию. Разработаны решения для Windows, Mac, Linux/Unix, Android. Сетевое приложение разработано на языках C, C++, Phyton, маршрутизация осуществляется с помощью распределенной сети серверов нодов (англ. Onion Routers), также называемыми многослойными маршрутизаторами, управляющими передачей трафика по магистральным сетям в зашифрованном виде. По состоянию на август 2013 года Tor включает в себя сеть из 4200 нодов, находящихся в разных местах планеты [14].

По мнению разработчиков, применение Tor в совокупности с другими методами защиты позволяет не только снизить до абсолютного минимума вероятность атак типа «man-in-the-middle» и предлагает эффективные средства защиты от программы разведки PRISM [15]. Луковая маршрутизация может стать эффективным решением для систем разных форматов с повышенными требованиями к безопасности. Несмотря на значительно более низкие риски атаки на Tor, их нельзя полностью исключить по причине - точки выхода и их IP-адреса опубликованы [16]. Для коммерческих систем безопасности возможности Tor вполне самодостаточны, через маршрутизаторы обрабатывается огромный объем информации, в которой достаточно сложно выделить объект шпионажа.

Защита трафика в пиринговых сетях. В заключение следует упомянуть унаследованные уязвимости пиринговых сетей. Существует ряд высокозащищенных архитектурных пиринговых решений, не относящихся к теме данного исследования.

Модель динамической защиты в прикладной конвергентной инфраструктуре и облачной среде. На текущий момент отсутствует общепринятая модель конвергентной инфраструктуры и облачной среды, что

затрудняет создание модели безопасности. В источнике [18] предложена агрегированная модель на базе анализа существующих конвергентных решений. Для конвергентной инфраструктуры характерно три слоя виртуализации: аппаратной виртуализации «на голом железе» низкопроизводительных и высокопроизводительных ресурсов, взаимный доступ к которым обеспечивается за счет сервисного слоя виртуализации, представленным федерацией облаков.

Базовой технологической компонентой конвергентной инфраструктуры является вычислительная ткань (англ. Fabric computing), которая реализует принцип многослойной организации инфраструктуры и представляет собой аппаратную и логическую виртуализацию ресурсов с топологиями: в высокопроизводительном сегменте - «server-to-server», «storage-to-storage»; в низкопроизводительном – «machine-to-machine», «peer-to-peer», в слое виртуализации предложены ткани типа «cloud-to-cloud», а для соединения конвергентных решений «fabric-to-fabric».

Средства динамической защиты реализуются с помощью облачной платформы, включающей классические и дополнительные подсистемы безопасности (акселератор соединений). Для улучшения параметров достаточной безопасности реализуется принцип «одно облако – один сервис». К фичам предлагаемой прикладной конвергентной инфраструктуры типа IoT относится: анонимизация и шифрование трафика с помощью луковой (многослойной) маршрутизации с реализацией ткани NodeFabric серверов (нодов) со скрытыми IP-адресами в высокопроизводительном сегменте с топологией «node-to-node», а также принцип многослойного (перекрестного) сканирования инфраструктуры с помощью метода «колец безопасности» (см. источник [17]), слоев изолированных друг от друга, в которых требуется достижения параметра «достаточной безопасности» рис. 1.

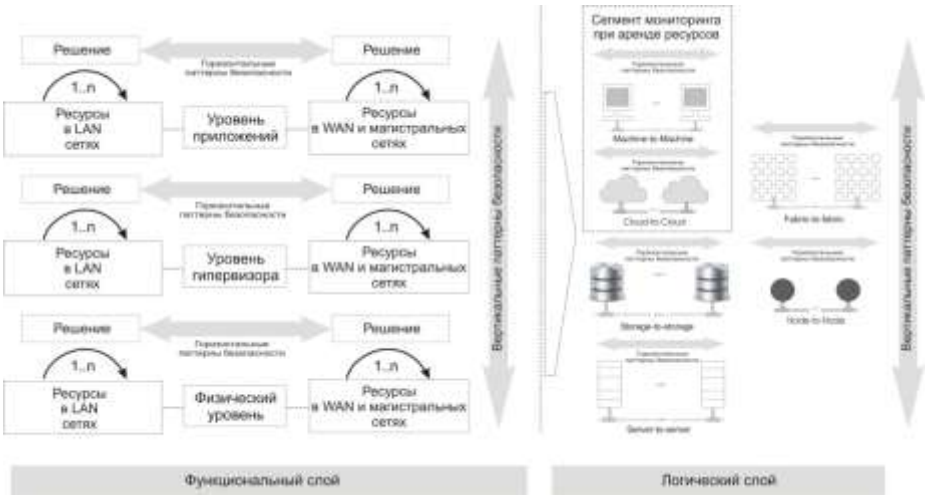

Рис. 1. Модель организации динамической защиты с использованием «колец безопасности» в прикладной конвергентной инфраструктуре

Использование интеллектуальных функций порождает свой набор уязвимостей, поэтому используемые смарт-функции максимально упрощены и реализованы не во всей системе, а каждом отдельном кольце безопасности. Каждое отдельное кольцо безопасности ткани реализовано на трех функциональных уровнях (физическом уровне, уровне гипервизора и уровне приложения) и множестве уровней виртуализации – вычислительных тканях различных топологий.

При разработке IoT-приложений на условиях аренды высокопроизводительных ресурсов для анонимизации и шифрования трафика применяется публичная луковая маршрутизация Tor для сокрытия местонахождения арендованных обслуживающих мощностей и IoT-устройств. В данном случае особое внимание уделяется безопасности трафика в магистральных сетях при сохранении набора упомянутых средств динамической защиты, реализованной в облачном слое, кольца безопасности образуют IoT-устройства на физическом слое, а функциональные сервисы – на физическом слое, уровне гипервизора и API, уровне приложения, обеспечивается безопасность других логических слоев. По похожему принципу может быть настроена надежность объектов при объектно-ориентированном программировании, сервисов – при сервисно-ориентированном и т.д. Задача будет стоять в разрешении конфликтов между категориями «колец безопасности».

Выводы и результаты исследования. Конвергентная инфраструктура является динамической средой, что требует реализации

динамических средств защиты с адаптивными метамоделями. Для систем общего назначения, управляющими IoT-устройствами, может быть применена платформа динамической защиты Akamai Intelligent Platform или Steelhead Cloud Accelerator, а для повышения уровня защищенности и сокрытия местоположения устройств – анонимизация и шифрование трафика на базе сети Tor. Отдельное внимание должно уделяться выбору используемой в IoT-системе виртуальной машины, наиболее защищенной на данный момент и сертифицированной по EAL5+ является XenSource от Citrix.

Системы специального назначения требуют более высокого уровня защиты. Для его повышения рекомендуется использование метода «колец безопасности» и перекрестного сканирования инфраструктуры, разработанного IBM-Zurich, с разработкой приприетарной системы динамической защиты. Платформа мониторинга предназначена динамично отслеживать угрозы, уязвимости, состояние веб-среды, загрузку ядер процессоров, управлять и оптимизировать трафик в LAN, WAN и магистральных сетях, а также анонимизировать трафик с помощью луковой маршрутизации. При создании прикладной конвергентной инфраструктуры для особо важных объектов представляется возможным развертывание собственной сети анонимизации трафика на базе луковой маршрутизации и ткани NodeFabric. Такое решение позволит использовать конвергентную инфраструктуру для IoT-решений специального назначения.

Литература

1. John Gantz, David Reinsel, «Extracting Value from Chaos», IDC, 2011 [Electronic resources]. – http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf .

2. Global Internet Traffic Projected to Quadruple by 2015, Cisco, 2012 [Electronic resources]. – http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003.

3. CiscoVisual Networking Index (VNI)Global IP Traffic Forecast Update; 2010–2015, Cisco, Sept 2011 [Electronic resources]. – http://www.ieee802.org/3/ad_hoc/bwa/public/sep11/nowell_01_0911.pdf.

4. Cisco VNI Global IP Traffic Forecast, 2012 – 2017, Cisco, May 2013 [Electronic resources]. – http://www.youtube.com/watch?v=tKDAUngzpbE.

5. Cisco VNI Service Adoption Forecast, 2012–2017, Cisco, 2013 [Electronic resources]. – http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1186/Cisco_VNI_SA_Forecast_WP.pdf.

6. Lindsay Hiebert, «Cisco's IOT Connected Safety and Security applications at Cisco Live», Blogs Cisco, June 2013[Electronic resources]. – http://blogs.cisco.com/?p=118486.

7. Jim Feldhan, «The Internet of Things: The Next Wave», Semico Research Corporation, May 2013 [Electronic resources]. – http://www.semico.com/content/internet-things-next-wave.

8. IBM X-Force 2012 Annual Trend and Risk Report, IBM, March 2013 [Electronic resources]. – http://www.ibm.com/ibm/files/I218646H25649F77/Risk_Report.pdf.

9. Appendix B: Security, VMware Security Certifications, Common Criteria, VMware. – Mode access: http://download3.vmware.com/vcat/vcat31_documentation_center/index.html#page/Architecting%2520a%2520vCloud/3a%2520Architecting%2520a%2520VMware%2520vCloud.2.140.html#wwpID0E04K0HA. : Common Criteria

10. Certified Products, Common Criteria. – Mode access: http://www.commoncriteriaportal.org/products/.

11. Akamai Intelligent Platform, Any experience. Any device. Anywhere. Akamai. – Mode access: http://www.akamai.com/html/technology/index.html.

12. Akamai Solution, Steelhead Cloud Accelerator, Akamai. – Mode access: http://www.akamai.com/html/solutions/steelhead_cloud_accelerator.html.

13. AKAMAI и RIVERBED разрабатывают совместное инновационное решение для ускорения работы SAAS, "Storage News" journal, Feb 2012 [Electronic resources]. – http://storagenews.ru/news_take.asp?Code=291.

14. Tor Metrics Portal: Network, Interactive graphs of relays in the network, Tor. – Mode access: https://metrics.torproject.org/network.html.

15. PRISM vs Tor, Tor, June 2013 [Electronic resources]. – https://blog.torproject.org/blog/prism-vs-tor.

16. Tor Network Status, Torstatus.Blutmagie. – Mode access: http://torstatus.blutmagie.de/.

17. Aurélien Wailly, Marc Lacoste, Hervé Debar «Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources», **IBM Research – Zurich, 2011** [Electronic resources]. - http://www.zurich.ibm.com/~cca/csc2011/submissions/wailly.pdf.

18. Луговой А.В., Зеленцова Ж.Ю. Анализ архитектуры глобальных конвергентных решений и синтез агрегированной модели. // Вестник Кременчугского национального университета. – 2013. – Вып. 3/2013 (80).– С. 84–91.

References

1. John Gantz, David Reinsel, «Extracting Value from Chaos», IDC, 2011 [Electronic resources]. – http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf .

2. Global Internet Traffic Projected to Quadruple by 2015, Cisco, 2012 [Electronic resources]. – http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003.

3. CiscoVisual Networking Index (VNI)Global IP Traffic Forecast Update; 2010–2015, Cisco, Sept 2011 [Electronic resources]. – http://www.ieee802.org/3/ad_hoc/bwa/public/sep11/nowell_01_0911.pdf.

4. Cisco VNI Global IP Traffic Forecast, 2012 – 2017, Cisco, May 2013 [Electronic resources]. – http://www.youtube.com/watch?v=tKDAUngzpbE.

5. Cisco VNI Service Adoption Forecast, 2012–2017, Cisco, 2013 [Electronic resources]. – http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns1186/Cisco_VNI_SA_Forecast_WP.pdf.

6. Lindsay Hiebert, «Cisco's IOT Connected Safety and Security applications at Cisco Live», Blogs Cisco, June 2013[Electronic resources]. – http://blogs.cisco.com/?p=118486.

7. Jim Feldhan, «The Internet of Things: The Next Wave», Semico Research Corporation, May 2013 [Electronic resources]. – http://www.semico.com/content/internet-things-next-wave.

8. IBM X-Force 2012 Annual Trend and Risk Report, IBM, March 2013 [Electronic resources]. – http://www.ibm.com/ibm/files/I218646H25649F77/Risk_Report.pdf.

9. Appendix B: Security, VMware Security Certifications, Common Criteria, VMware. – Mode access: http://download3.vmware.com/vcat/vcat31_documentation_center/index.html#page/Architecting%2520a%2520vCloud/3a%2520Architecting%2520a%2520VMware%2520vCloud.2.140.html#wwpID0E04K0HA. : Common Criteria

10. Certified Products, Common Criteria. – Mode access: http://www.commoncriteriaportal.org/products/.

11. Akamai Intelligent Platform, Any experience. Any device. Anywhere. Akamai. – Mode access: http://www.akamai.com/html/technology/index.html.

12. Akamai Solution, Steelhead Cloud Accelerator, Akamai. – Mode access: http://www.akamai.com/html/solutions/steelhead_cloud_accelerator.html.

13. AKAMAI i RIVERBED razrabatyvajut sovmestnoe innovacionnoe reshenie dlja uskorenija raboty SAAS, "Storage News" journal, Feb 2012 [Electronic resources]. – http://storagenews.ru/news_take.asp?Code=291.

14. Tor Metrics Portal: Network, Interactive graphs of relays in the network, Tor. – Mode access: https://metrics.torproject.org/network.html.

15. PRISM vs Tor, Tor, June 2013 [Electronic resources]. – https://blog.torproject.org/blog/prism-vs-tor.

16. Tor Network Status, Torstatus.Blutmagie. – Mode access: http://torstatus.blutmagie.de/.

17. Aurélien Wailly, Marc Lacoste, Hervé Debar «Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources», IBM Research – Zurich, 2011 [Electronic resources]. - http://www.zurich.ibm.com/~cca/csc2011/submissions/wailly.pdf

.

18. Lugovoj A.V., Zelencova Zh.Ju. Analiz arhitektury global'nyh konvergentnyh reshenij i sintez agregirovannoj modeli. // Vestnik Kremenchugskogo nacional'nogo universiteta. – 2013. – Vyp. 3/2013 (80).– S. 84–91.

Зеленцова Ж.Ю., Луговой А.В.

УРАЗЛИВОСТІ КОНВЕРГЕНТНОЇ ІНФРАСТРУКТУРИ ТА ПРАКТИЧНІ ПІДХОДИ ДО ЇХ УСУНЕННЯ

Проведено агрегований аналіз загроз у конвергентної інфраструктурі з метою створення захищених прикладних конвергентних систем моніторингу для IoT-пристроїв. Практичні підходи щодо забезпечення безпеки розглянуті на моделі розгортання.

Ключові слова: *уразливості конвергентної інфраструктури, методи захисту хмар.*

Lugovoi A., Zelentsova ZH.

CRITICAL CONVERGED INFRASTRUCTURE VULNERABILITY AND PRACTICAL APPROACHES TO THEIR ELIMINATION

The article analyzed the vulnerability of critical converged infrastructure and methods for their elimination. The results are shown by the deployment model of a dynamic system cloud security.

Keywords: *vulnerability of converged infrastructure, cloud security.*

Зеленцова Ж.Ю., соискатель, Кременчугский национальный университет имени Михаила Остроградского.

Луговой А.В., к.т.н., проф., заведующий кафедрой «Компьютерные информационные системы», КрНУ, Кременчугский национальный университет имени Михаила Остроградского.

Рецензент: Скопа А.А. д.т.н., проф., заведующий кафедрой «Информационные системы в экономике» Одесского национального экономического университета, г. Одесса.