УДК - 004.056 + 005.334:004.056 Вестник УрФО № 1(23) / 2017, с. 14–19

Баринов А.Е., Рябцева О.В., Соколов А.Н.

АДАПТИВНАЯ ОЦЕНКА КЛИЕНТСКОГО РИСКА В ОБЛАЧНЫХ ИНФРАСТРУКТУРАХ

В статье описаны основные угрозы облачных инфраструктур согласно стандарту NIST. Рассмотрена проблема оценки риска для клиента, использующего облачные инфраструктуры. Описаны ранее существующие подходы и стандартные модели. В статье предложено совместное использование статистического подхода и CVSS 3.0 оценок уязвимостей в программных продуктах для расчёта вероятности компрометации облачного сервиса. Использованный подход предполагает проведение отдельных оценок для вероятности и критичности возникновения рисков целостности, конфиденциальности и доступности. Описан метод итоговой оценки риска для клиента и рекомендации по его использованию.

Ключевые слова: *облачные вычисления, информационная безопасность, уязвимость, оценка риска.*

Barinov A.E., Ryabtseva O.V., Sokolov A.N.

ADAPTIVE CUSTOMER RISK ASSESSMENT IN CLOUD INFRASTRUCTURE

The paper is described the main security threats to cloud infrastructures according to NIST standard. The problem of risk assessment for a client using cloud infrastructure is considered. Previous approaches and standard models are described. The article proposes the joint use of the statistical approach and CVSS 3.0 vulnerability assessment in software products to calculate the disadvantages of compromising the cloud service. The approach involves a variety of assessments of the probability and severity of the occurrence of risks of integrity, confidentiality and availability. The method of final risk assessment for the client and recommendations for its use are described.

Keywords: *cloud computing, information security, vulnerability, risk assessment.*

Облачные вычисления - это модель обеспечения удобного повсеместного сетевого доступа по требованию к совместно используемому пулу конфигурируемых вычислительных ресурсов, которые можно быстро предоставить и внедрить с минимумом административных усилий или взаимодействия с сервис-провайдером.

Защита данных является важной проблемой, особенно для ресурсов облачного типа, предоставляемых дистанционно широкому кругу клиентов. Решение использования одних и тех же компьютеров, и программного обеспечения для разных целей разными пользователями является экономически обоснованным, но данный подход требует повышенного внимания к безопасности и разграничению прав, а также к балансировке нагрузки на аппаратную часть.

Модели обслуживания взаимосвязаны между собой вложенностью типов подписки IaaS-PaaS-SaaS. Таким образом, проблемы информационной безопасности для разных моделей сервиса в облаке имеют взаимосвязанный характер. То есть, при уязвимости на любом нижележащем, например уровне (IaaS), проблемы будут наследоваться и на более высокие слои.

Существуют несколько ведущих организаций, которые занимаются вопросами безопасности в облачных инфраструктурах:

– Альянс безопасности в «облаке» (Cloud Security Alliance, CSA);

– Европейское агентство сетевой и информационной безопасности (ENISA);

– Национальный институт стандартов и технологий (NIST).

Стандарт безопасности облачных вычислений (NIST Cloud Computing Security Reference Architecture), принятый в NIST, охватывает возможные потенциальные типы атак на сервисы облачных вычислений[1]:

– компрометация конфиденциальности и доступности данных, передаваемых облачными провайдерами;

– атаки, которые исходят из особенностей структуры и возможностей среды облачных вычислений для усиления и увеличения ущерба от атак;

– неавторизированный доступ потребителя (посредством некорректной аутентификации или авторизации, или уязвимостей, внесенных посредством периодического технического обслуживания) к ПО, данным и ресурсам, используемым авторизированным потребителем облачного сервиса;

– увеличение уровня сетевых атак, таких как DoS, эксплуатирующих ПО, при разработке которого не учитывалась модель угроз для распределенных ресурсов интернета, а также уязвимости в ресурсах, которые были доступны из частных сетей;

– ограниченные возможности по шифрованию данных в среде с большим количеством участников;

– переносимость, возникающая в результате использования нестандартных API, которые усложняют облачному потребителю возможность перехода к новому облачному провайдеру, когда требования доступности не выполняются;

– атаки, эксплуатирующие физическую абстракцию облачных ресурсов и недостатки в записях и процедурах аудита;

– атаки на виртуальные машины, которые не были соответствующим образом обновлены;

– атаки, эксплуатирующие нестыковки в глобальных и частных политиках безопасности.

Также стандарт выделяет основные задачи безопасности для облачных вычислений. Однако, наиболее специфическими для облачных инфраструктур являются следующие:

– защита от «цепных» (supply chain threats) угроз, включающая в себя подтверждение степени доверия и надежности сервис провайдера в той же степени, что и степень доверия используемого ПО и оборудования;

– задание доверенных границ между сервис-провайдером и потребителями для того, чтобы убедиться в ясности авторизованной ответственности за предоставление безопасности;

– поддержка переносимости, осуществляемой для того, чтобы потребитель имел возможность сменить облачного провайдера в тех случаях, когда у него возникает необходимость в части удовлетворения требований по целостности, доступности, конфиденциальности, включающая в себя возможность закрыть аккаунт в данный момент и копировать данные от одного сервис-провайдера к другому.

При этом стандарт NIST не описывает методик расчёта риска для облачных инфраструктур, а только перечисляет компоненты обеспечения безопасности в облачных инфраструктурах и уровни, на которых они должны быть реализованы, а также коэффициенты критичности для целостности, конфи-

денциальности и доступности для основных сценариев использования облачных технологий[1].

Стандарт ENISA[4] описывает 35 типовых сценариев развития рисков в облачных инфраструктурах, сопутствующие факторы их развития и подверженные рискам активы, оценивает вероятность и критичность каждого из них, предлагает модель оценки риска. Однако каждый из этих сценариев описан автономно. Стандарт не предполагает совместного развития сценариев и гибкой оценки риска для пользователей облачных ресурсов. Данное обстоятельство породило множество научных работ[2,3,5,6], посвящённых адаптивной оценке риска в облачных инфраструктурах. Но в современных источниках не дается исчерпывающее решение, которое обеспечивает адаптивную оценку риска для каждого клиента облачной инфраструктуры, а также обеспечивающую объективную оценку риска для клиента, защищённую от вмешательства сервис-провайдера. Известный подход[2] предполагает под собой оценку взаимного влияния программных компонентов на риск эксплуатации уязвимости и позволяет адаптивно рассчитать индекс безопасности для каждого клиента в зависимости от целей в обеспечении безопасности. Однако для его реализации требуется значительный ручной ввод экспертной информации, что повышает вероятность ошибочной оценки. Кроме того, в описываемом программном средстве отсутствует возможность интеграции с системой обнаружения уязвимостей. В другом известном подходе[3] описывается модель взаимного влияния уязвимостей в облачных инфраструктурах, однако она предполагает под собой небольшой набор из 15 правил взаимного влияния уязвимостей в программных компонентах для стандартного стека ПО. Данная модель не предполагает под собой детерминированную оценку риска для различных по критичности для разного типа угроз активов пользователей, использующих один и тот же стек ПО.

Подход[6] использует в качестве основы сценарии рисков ENISA[4], однако, для оценки вероятности возникновения угрозы использует методику на основе опросника CAIQ[7], что позволяет выполнить только экспертную оценку без учёта технических рисков, вызванных уязвимостями в программном обеспечении. Соответственно, даже при появлении технического описания уязвимости в открытых базах, невозможно оценить риск её влияния на конкретного пользователя облачной инфраструктуры.

Модель JRTM[5] (Joint Risk and Trust Model) предполагает оценку риска в зависимости от накопленной статистики сервис-провайдера по возникновению и устранению уязвимостей; оценку риска при наличии нескольких компонентов разной степени критичности и вероятности эксплуатации уязвимости, как у сервис-провайдера, так и у пользователя. Однако она не предполагает адаптацию оценки риска в зависимости от статуса уязвимости (наличие официального исправления, временного решения и т.д.), а также зрелости эксплойта и степени доступности информации об уязвимости. Также данная модель рассчитывает только вероятности возникновения угроз, вызванных уязвимостями, не учитывая степень их влияния на инфраструктуру, а также оценки степени риска уязвимостей из общедоступных баз CVE, DWF и других.

Рассмотрим выражение, для риска предложенное в модели JRTM:

$$\delta_f = r_f(1 - t_f) \quad (1)$$

Здесь указанная вероятностная оценка риска, состоящая из двух компонент r_f - вероятности возникновения угрозы, вызванной уязвимостью и t_f - вероятностью устранения уязвимости сервис-провайдером до тех пор, пока она не приведёт к инциденту информационной безопасности. Здесь и далее индекс $f \in \{\varepsilon; \phi; \rho\}$, что означает соответственно значения, относящиеся к целостности, конфиденциальности и доступности. При этом значение вероятности возникновения угрозы оценивается как:

$$r_{f(i)} = (1 - \omega)R(f) + \omega\frac{f_i}{u_i} \quad (2)$$

где $R(f)$ случайная величина, основанная на функциях распределения вероятности, полученных из статистического анализа наблюдений за возникающими уязвимостями целостности, конфиденциальности и доступности. Модель JRTM является дискретной моделью и рассматривает время как набор периодов равной длины, где i – номер периода, а f_i - соответствующее ему количество клиентов сервис-провайдера, у которых возникла в этом периоде хотя бы одна уязвимость соответствующего типа, а u_i - суммарное количество клиентов, $\omega \in [0;1]$ - экспертная весовая оценка роли последнего периода.

Вероятность устранения уязвимости сервис-провайдером до тех пор, пока она не приведёт к инциденту информационной без-

опасности в работе[5] оценивается как:

$$t_f = \begin{cases} 0, & t_{sf} < 0 \\ 1, & t_{sf} > 1 \\ t_{sf}, & t_{sf} \in [0;1] \end{cases} \quad (3)$$

.

Оценка вероятности устранения уязвимости сервис-провайдером состоит из двух составляющих, основанных на долговременной статистике t_{fh} и кратковременной t_{fs} - за два последних периода, то есть:

$$t_{sf} = t_{fh} + t_{fs}, \quad (4)$$

Где долговременные оценки. вычисляются аналогично вероятности возникновения уязвимости:

$$t_{\varepsilon h(i)} = (1-\omega)R(\varepsilon_e) + \omega\frac{\varepsilon_{ei}}{\varepsilon_i}, \quad (5)$$

$$t_{\rho h(i)} = (1-\omega)R(\rho_e) + \omega\frac{\rho_{ei}}{\rho_i}, \quad (6)$$

$$t_{\phi h(i)} = \left((1-\omega)R(\phi_e) + \omega\frac{\phi_{ei}}{\phi_i}\right)^{R(D)} \quad (7)$$

.

Стоит отметить, что соответствующие значения f_{ei} - число клиентов, для которых уязвимости соответствующего типа, были предотвращены до того, как это повлекло возникновение инцидента в i периоде. $R(f_e)$ - соответствующие статистические распределения. В оценке конфиденциальности дополнительно включено распределение; $R(D)$, характеризующее количество периодов в течении которого существуют уязвимости конфиденциальности, то есть периодов течении которых возможна утечка информации.

Кратковременная оценка формируется как:

$$t_{fs(i)} = \begin{cases} d_{f(i)}^{\gamma}, & d_{f(i)} \geq 0 \\ -\sqrt[\gamma]{|d_{f(i)}|}, & d_{f(i)} < 0 \end{cases} \quad (8)$$

,

$$d_{f(i)} = \frac{f_{ei}}{f_i} - \frac{f_{e(i-1)}}{f_{i-1}} \quad (9)$$

.

где $\gamma \geq 1$ - экспертная тенденциозная оценка динамики деятельности провайдера по реакции на уязвимости.

При этом выражение (4) в работе[5] предполагает, что все уязвимости каждого класса устранимы за одинаковое время, однако уязвимости в программных продуктах могут иметь готовое решение для исправления, выпущенное производителем, либо временное решение, которое, возможно, должен реализовать провайдер, либо не иметь ничего из вышеперечисленного. Кроме того уязвимости могут иметь известный эксплойт, принцип его построения или не иметь такового. Зрелость эксплойта, уровень известности уязвимости, а также доступности её исправления влияют на скорость реакции сервис-провайдера по её исправлению, а также вероятность её эксплуатации. Используемый для оценки критичности уязвимостей в открытых базах стандарт CVSS 3.0[8] оценивает параметры: доступности исправления $t_{rl} \in [0.95;1]$ (нижнее значение – официальное исправление, верхнее его отсутствие или неизвестность его существования); зрелости эксплойта $t_{em} \in [0.91;1]$ (нижнее значение – наличие существования эксплойта не доказано, верхнее – имеется работоспособная версия); уровня доступности информации об уязвимости $t_{rc} \in [0.92;1]$ (нижнее значение – общедоступная информация об уязвимости не содержит технических деталей, верхнее – доступно детальное описание уязвимости). Ведение отдельной статистики по устранению различных категорий уязвимостей, значительно усложнит теоретический аппарат, кроме того в течение своего жизненного цикла уязвимость неоднократно меняет указанные выше параметры. Поэтому предлагается выполнять оценку t_{sf} как

$$t_{sf} = t_{fh} + t_{fs} + \sum_{j=1}^{n} 1 - t_{rlj} t_{emj} t_{rcj}. \quad (10)$$

В выражении (10) предполагается, что клиент или облачный провайдер подвержены одновременно n уязвимостям.

Если число сервисов используемых клиентом m, то его суммарная оценка вероятности возникновения инцидента[5]:

$$\varepsilon = 1 - \prod_{k=1}^{m} (1 - \delta_{\varepsilon m}), \quad (11)$$

$$\phi = 1 - \prod_{k=1}^{m} (1 - \delta_{\phi m}), \quad (12)$$

$$\rho = 1 - \prod_{k=1}^{m} \left(1 - \prod_{z=1}^{a_k} \delta_{\rho kz}\right). \quad (13)$$

Оценка доступности ρ отличается тем, что введён дополнительный параметр a_k - означающий общее количество сервисов или оборудования на которых может быть реализован тот же функционал клиента. Однако существует множество моделей[9,10] обеспечения и оценки доступности и данный вопрос заслуживает отдельной работы.

Фактор критичности уязвимостей для клиента может быть выражен, как:

$$I_{fs} = 1 - \prod_{k=1}^{n} (1 - I_{fk}) \quad , \qquad (14)$$

где I_{fk} - оценка критичности для целостности, конфиденциальности или доступности для соответствующей уязвимости в ПО. Данные значения содержаться в описании уязвимости по стандарту CVSS 3.0.

Тогда суммарный риск C_f можно выразить как совместную оценку его влияния и вероятности возникновения[6] или

$$C_{fs} = \frac{\lfloor 10 I_{fs} \rfloor + \lfloor 10 f \rfloor}{18} \quad . \qquad (15)$$

Суть (15) в том, что рейтинг маловероятных и малокритичных уязвимостей относительно снижается.

Для разных сервисов и разных клиентов возможны разные оценки критичности для разных составляющих информационной безопасности. Их клиент может оценить на основе своих бизнес-требований или опираясь на рекомендации, например[1]. Тогда в качестве итоговой оценки влияния уязвимостей можно получить следующее выражение:

$$C_s = 1 - (1 - C_\varepsilon R_\varepsilon)(1 - C_\phi R_\phi)(1 - C_\rho R_\rho) \, , \qquad (16)$$

где R_ε, R_ϕ, R_ρ - соответствующие оценки критичности целостности, конфиденциальности и доступности, связанные следующим соотношением:

$$R_\varepsilon + R_\phi + R_\rho = 1 \quad . \qquad (17)$$

Выражение (16) может быть применено клиентами облачных инфраструктур для оценки безопасности своих сервисов использующих облачные инфраструктуры сервис-провайдеров. Данные оценки могут быть получены, как для всего сервиса клиента, так и для каждого отдельно взятого используемого им сервис-провайдера, что может быть им использовано для выбора оптимального расположения ресурсов своих сервисов с точки зрения информационной безопасности при наличии нескольких сервис-провайдеров. Недостатками подхода является то, что во-первых статистические данные для выражений (2)-(9) может поставлять только сервис-провайдер с помощью системы мониторинга, следовательно здесь встаёт вопрос об обеспечении доверия к данным провайдера. Во – вторых, как отмечалось выше, возможно существование различных схем резервирования провайдеров, и для более точных оценок доступности этот факт следует учитывать.

Статья выполнена при поддержке Правительства РФ (Постановление №211 от 16.03.2013 г.), соглашение № 02.A03.21.0011.

Примечания

[1] NIST Cloud Computing Security Reference Architecture, National Institute of Standards and Technology, Special Publication 500-299, May 2013.

[2] D. Dasgupta and M. Rahman, "A framework for estimating security coverage for cloud service insurance," in Proceedings of the 7th Annual Cyber Security and Information Intelligence ResearchWorkshop: Energy Infrastructure Cyber Protection (CSIIRW '11), Oak Ridge, Tenn, USA, October 2011

[3] I. Khalil, A. Khreishah, M. Azeem, Cloud computing security: a survey, Comput. (MDPI J.) 3 (1) (2014) 1–35, http://dx.doi.org/ 10.3390/computers3010001

[4] Cloud Computing: Benefits, risks and recommendations for information security, ENISA, November 2009

[5] Erdal Cayirci, Models for Cloud Risk Assessment: A Tutorial. Accountability and security in cloud, Springer April 2015, Vol. 8937 of series lecture notes in computer science, pp 154-184

[6] Cayirci, E., Garaga, A., Santana de Oliveira, A. et al. J Cloud Comp (2016) 5: 14. doi:10.1186/s13677-016-0064-x

[7] https://cloudsecurityalliance.org/group/consensus-assessments/

[8] Common Vulnerability Scoring System v3.0: Specification Document (v1.7)

[9] Availability Management Framework - Application Interface Specification SAI-AIS-AMF-B.04.01.

[10] Gonçalves G, Endo P, Rodrigues M, Sadok D, Curesco C Risk-based model for availability estimation of saf redundancy models. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7543848

Баринов Андрей Евгеньевич, аспирант кафедры инфокоммуникационные технологии, старший преподаватель кафедры защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)». 454080, г. Челябинск, пр. Ленина, 76. E-mail: barinovae@susu.ru.

Barinov Andrey, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: barinovae@susu.ru.

Рябцева Ольга Викторовна, студентка ФГАОУ ВО «Южно-Уральский государственный университет» (национальный исследовательский университет). 454080, г. Челябинск, пр. Ленина, 76. E-mail: olyska33@mail.ru.

Ryabtseva Olga, student, "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: olyska33@mail.ru.

Соколов Александр Николаевич, кандидат технических наук, доцент, заведующий кафедрой защиты информации ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», г. Челябинск. E-mail: SokolovAN@susu.ru.

Sokolov Alexander, Federal State Autonomous Educational Institution of Higher Education "South Ural State University (national research university)", Chelyabinsk, Russian Federation. E-mail: SokolovAN@susu.ru.