Политика проведения оценки защищённости и тестирования на уязвимости

ООО «Облачные технологии»

Общие положения

Настоящая Политика проведения оценки защищённости и тестирования на уязвимости (далее – Политика) ООО "Облачные технологии" (далее – Cloud.ru) разработана с целью определения условий, требований и ограничений проведения проверки информационных систем (далее – ИС) клиентами сервисов Cloud.ru, а также третьими лицами, привлечёнными для выполнения данных работ.

Цели Политики

Целями настоящей Политики являются:

- Обеспечение единого подхода к проведению проверок в рамках сервисов, предоставляемых Cloud.ru.

- Минимизация рисков повреждения ИС и утечки конфиденциальной информации в процессе проведения проверок.

- Определение ответственности и обязанностей всех участников процесса проверок.

Область применения

Положения Политики обязательны к исполнению всеми клиентами Cloud.ru и применимы к любым действиям, направленным на анализ безопасности, включая автоматизированные и ручные методы тестирования.

Термины и определения

Cloud.ru – ООО «Облачные технологии», расположенное по адресу: 117312, г. Москва, ул. Вавилова, д.23, стр.1, комната №1.207; ИНН: 7736279160; ОГРН: 5167746080057.

DDoS – Distributed Denial of Service, распределенная атака типа «отказ в обслуживании».

DNS – компьютерная распределенная система для получения информации о доменах. Используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и (или) обслуживающих узлах для протоколов в домене (SRV-запись).

IP-адрес – уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

LDAP – (Lightweight Directory Access Protocol) протокол/набор правил и соглашений, которые определяют, как будут передаваться и приниматься данные.

Автоматизированный метод тестирования – проверка программного обеспечения с помощью специальных инструментов.

Аккаунт – хранимая в системе Исполнителя совокупность данных и настроек для обеспечения

Заказчика возможностью управлять количеством и функционалом потребляемых Услуг. Аккаунт позволяет обеспечить корректное взаимодействие Заказчика со службами Технической поддержки Исполнителя.

Виртуальная машина – виртуальный аналог физического компьютера, на котором можно запускать ОС, приложения, сервисы и выполнять те же функции, что и на физическом оборудовании.

Договор – договор-оферта на оказание услуг, размещенный на сайте Общества в информационно-телекоммуникационной сети-Интернет по адресу https://www.cloud.ru/documents/.

Инфраструктура – совокупность Технологических площадок, информационных систем, баз данных, каналов связи, а также программного обеспечения (программ для ЭВМ) Исполнителя, обеспечивающая надлежащее оказание Услуг.

Инцидент – незапланированное событие, которое привело или может привести к недоступности или снижению качества предоставления Услуг.

ИС – информационная система.

Клиент – юридическое или физическое лицо, которое пользуется услугами Cloud.ru.

Конечный пользователь (заказчик) – заказчик, т.к. он является фактическим конечным пользователем (потребителем) ПО.

Недоступность Услуг – зафиксированный факт невозможности использования Заказчиком основной функциональности Услуги.

Организация – сущность, которая, содержит полную информацию о компании-клиенте: договор, используемые платформы и сервисы, лимит расходов, статистические данные о потребленных услугах и оплате, список пользователей и распределение их по структурным единицам организации.

ОС – операционная система, комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Пассивное сканирование – метод сбора информации о целевой системе или сети без активного взаимодействия с ней.

Платформа – совокупность сервисов, программных и/или аппаратных средств, решающая определенную задачу или группу задач.

ПО – программное обеспечение, программа для ЭВМ, Программный продукт.

Политика – правило или набор правил, которые позволяют предоставлять разным группам Пользователей единый набор прав при взаимодействии с Личным кабинетом, иными словами, распределять единообразные Роли среди групп Пользователей.

Пользователь – лицо, осуществляющее непосредственное взаимодействие в Личном кабинете от имени и в интересах Заказчика в соответствии с Ролью или полномочиями, которыми Пользователя наделил Заказчик для администрирования Услуги.

Пользовательское соглашение – размещенное в интерфейсе Маркетплейса Cloud.ru соглашение, определяющее порядок использования Программных продуктов, размещенных на Маркетплейсе Cloud.ru, содержащее все существенные и необходимые условия для его

заключения с Пользователем.

Продукт – информационные системы, программное обеспечение, ИТ-сервисы,

предоставляемые клиентам за плату.

Ресурс – единица вычислительных, сетевых, хранения данных и других компонентов Услуг, доступ к которой предоставляется Заказчику посредством сети Интернет по его требованию для выполнения различных задач. Ресурсы включают, но не ограничиваются, такими элементами, как флейворы, экземпляры БД, диски и другие.

Ручной метод тестирования – процесс проверки программного продукта или приложения вручную, без использования автоматизированных инструментов.

Сервис – техническое решение, функциональность или вычислительный ресурс для решения определенной бизнес-задачи.

Третьи лица – любое юридическое или физическое лицо, не являющееся Аффилированным лицом одной из Сторон

Услуги – услуги, оказываемые Исполнителем Заказчику по Договору в соответствии с Приложениями 1 к Договору и Заказами.

Уязвимость – недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использован для реализации угроз кибербезопасности.

В область действия процесса управления уязвимостями попадают следующие типы уязвимостей:

- уязвимости разработки – уязвимость, появившаяся в процессе разработки программного обеспечения, для устранения которой требуется установка обновления или замена версии ПО;

- уязвимость конфигурации – уязвимость, появившаяся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы.

Эксплойт – программа, фрагмент кода или данных, которые предназначены для использования ошибки или уязвимости в приложении или операционной системе.

Требования к проведению проверок

Общие положения

Проведение оценки защищённости и проверки на уязвимости возможно исключительно в отношении ресурсов, **предоставленных** клиенту Cloud.ru.

Все работы должны выполняться с учётом положений настоящей Политики, действующего законодательства и пользовательского соглашения.

При проведении работ должны соблюдаться принципы обеспечения минимизации воздействия на инфраструктуру, обеспечения непрерывности бизнес-процессов и предотвращения влияния на других клиентов.

Любые действия, выходящие за рамки допустимого поведения, в том числе описанные в разделе Политики «Запрещенные действия», считаются нарушением условий использования сервисов

или услуг Cloud.ru.

Подготовка к проверке

Перед проведением работ клиент обязан предварительно направить заявку в техническую поддержку Cloud.ru по адресу support@cloud.ru не менее чем за 14 (четырнадцать) календарных дней до запланированного начала работ.

Заявка обязательно должно содержать:

1. Перечень с описанием запланированных работ;
2. идентификатор аккаунта и список сервисов, к которым будет осуществляться доступ;
3. список внешних статических IP-адресов, с которых будет производиться сканирование;
4. временные окна проведения работ;
5. контактные данные сотрудников клиента, выполняющих проверку, для оперативной связи, включая номер телефона ответственного лица.

Cloud.ru рассматривает заявку в течение 5 (пяти) рабочих дней и направляет клиенту решение.

Допустимые виды работ

Клиентам Cloud.ru разрешается самостоятельно либо с привлечением уполномоченных подрядчиков осуществлять следующие действия, при условии соблюдения настоящей Политики и полной гарантии отсутствия вреда для инфраструктуры Cloud.ru, других клиентов Cloud.ru и стабильности платформы:

1. Пассивное сканирование: сбор информации о собственных сервисах без активного взаимодействия (например, banner grabbing, анализ открытых метаданных);
2. **Автоматизированное сканирование на уязвимости: запуск неагрессивных сканеров*;**
3. Тестирование конфигурации: проверка правильности настроек собственных сервисов, включая валидацию SSL-сертификатов, заголовков безопасности, политик CORS и Content Security Policy;
4. Проверка авторизации и аутентификации: анализ процессов входа и управления сессиями в рамках собственных приложений;
5. **Оценка отказоустойчивости собственных приложений: моделирование неинтенсивных нагрузок на сервисы клиента**** без воздействия на платформенные компоненты Cloud.ru;
6. Верификация соответствия условий эксплуатации и SLA: тесты, направленные на измерение времени отклика, доступности и других параметров, не затрагивающие инфраструктуру Cloud.ru.

Любые действия, выходящие за рамки указанных выше типов проверок, подлежат отдельному согласованию.

Проведение любых проверок инфраструктуры Cloud.ru или данных иных клиентов за пределами разрешённых условий категорически запрещается.

***Неагресивные сканеры** - это инструменты для автоматизированного сбора информации и анализа уязвимостей, которые минимизируют воздействие на целевые системы. Они работают в "пассивном" или "тихом" режиме, избегая действий, которые могут вызвать отказ в обслуживании (DoS), блокировку IP или искажение данных.

Критерии неагрессивности:

- Низкая скорость запросов (например, --max-rate 10 в Nmap).
- Отсутствие эксплуатации уязвимостей (только обнаружение).
- Минимизация нагрузки (избегание параллельных соединений).
- Использование пассивных методов (анализ заголовков, DNS, SSL-сертификатов).

Примеры:

nmap -sS -T2 -Pn --max-rate 50 -p 80,443,22,21 <target>

-sS: SYN-сканирование (не завершает соединение).

-T2: режим "Polite", цель минимизировать нагрузку на целевую систему

--max-rate 50: ограничение пакетов в секунду.

nikto -h <target> -Tuning 1 -evasion 1

zap-cli quick-scan --spider --ajax-spider --start-options '-config scanner.attackStrength=Low' <URL>

****Оценка отказоустойчивости** — это процесс тестирования способности приложения сохранять работоспособность при умеренных нагрузках, без влияния на базовую инфраструктуру (например, платформенные компоненты Cloud.ru).

Ключевые аспекты и рекомендации:

- Тестируются только пользовательские приложения, без нагрузки на облачную платформу. Нагрузка дозированная, имитирует реальное использование (не стресс-тест).
- Проверяется:
  - Стабильность работы под нагрузкой.
  - Корректность обработки ошибок.
  - Влияние на смежные сервисы.
- Начинать с 1-5 RPS, затем плавно повышать до нагрузок не превышающих реальное используемые.

Ограничения:

1. Не затрагивать Cloud.ru:
2. Избегать DDoS-подобных сценариев.
3. Не тестировать платформенные сервисы (базы данных, брокеры сообщений).

Порядок проведения работ

Рекомендации по проведению работ

Для обеспечения корректного и безопасного проведения работ рекомендуется:

- использовать зарезервированный внешний статический IP-адрес, с которого осуществляется тестирование;

- вести журналирование (логирование) всех действий в хронологическом порядке (timeline), включая дату, время, скрипты и идентификаторы выполненных операций;

- использовать инструменты, позволяющие исключить Flood и агрессивные действия;

- предварительно протестировать инструменты, скрипты и сценарии в изолированной среде.

Правила проведения проверки уязвимостей клиента

Мероприятия по оценки могут включать в себя сканирование на уязвимости, тесты на проникновения, проверки соответствия условий эксплуатации.

Клиент может самостоятельно или с помощью подрядчиков оценить безопасность собственного программного обеспечения, если это не противоречит Политике.

Клиент обязан в установленный срок направить заявку Cloud.ru о предстоящих проверках, направив на адрес электронной почты (support@cloud.ru) заявку на проведение работ в соответствии с требованиями, изложенными в общих положениях.

Клиент до начала проведения мероприятий обязан получить ответ от Cloud.ru о возможности проведения проверки в соответствии с заявкой.

При обнаружении уязвимостей в инфраструктуре Cloud.ru, получении доступа к инфраструктуре, сервисам или данным другого клиента, непреднамеренном воздействии на сервисы Cloud.ru или третьих лиц, клиент обязан незамедлительно прекратить работы и в течение 2 часов уведомить об этом Cloud.ru, направив письмо на электронный адрес технической поддержки (support@cloud.ru).

Правила проведения сканирования ресурсов третьих лиц

В случае использования инфраструктуры Cloud.ru для проведения проверки в интересах сторонних организаций (третьих лиц), клиент обязан получить согласие Cloud.ru на соответствующие действия.

Проведение таких проверок допускается только при наличии:

1. Официального согласия владельца ресурсов, подлежащих проверке;
2. Согласованного плана работ с Cloud.ru;
3. Поданной в срок заявки и её согласования, в соответствии с требованиями, указанными в общих положениях.

Cloud.ru вправе запросить дополнительные подтверждения, включая договор между клиентом и конечным заказчиком проверки.

В случае непредоставления необходимых документов действия клиента считаются нарушением условий использования продуктов и сервисов Cloud.ru и могут повлечь ограничение или блокировку клиентского аккаунта.

В случае доступа без разрешения к данным или ресурсам третьих клиент несёт полную ответственность за нанесённый ущерб, обязуется возместить убытки и гарантирует конфиденциальность полученной информации.

Ответственность сторон

Клиент несёт ответственность за:

1. Выполнение требований настоящей политики;
2. Своевременное направление заявок;
3. Корректную конфигурацию и безопасное использование инструментов тестирования;
4. Действия привлечённых подрядчиков и их последствия;
5. Своевременное уведомление Cloud.ru в случае обнаружения инцидентов;
6. Возмещение убытков, понесённых Cloud.ru или иными сторонами в результате нарушения настоящей Политики;
7. Последствия, включая сбои или потерю данных в собственной инфраструктуре.

Cloud.ru оставляет за собой право отказать клиенту в проведении проверки, ограничить её параметры или прервать выполнение при возникновении угроз безопасности или стабильности для инфраструктуры и сервисов.

Cloud.ru вправе при выявлении нарушений Политики Cloud.ru вправе, без предварительного уведомления, заблокировать аккаунт клиента или виртуальную машину клиента, с которой осуществляются действия, нарушающие настоящую Политику, до устранения нарушений.

Запрещенные действия - любые противоправные цели, с нарушением действующего законодательства.

Клиентам Cloud.ru запрещено:

Проведение или имитация DDoS-атак (L3/L4/L7), включая:

- SYN Flood, UDP Flood, ICMP Flood, Teardrop, Smurf;
- атаки с усилением через сторонние сервисы (DNS, NTP, LDAP, Memcached и др.)

Неавторизованный доступ и обход ограничений в сервисах Cloud;

- Попытки обхода систем аутентификации или авторизации;
- Использование уязвимостей для эскалации привилегий;
- Любые действия, нарушающие положения договора между клиентом и Cloud.ru.

Массовые автоматизированные запросы

- Проведение нагрузочного тестирования или стресс-тестов без согласования;
- Использование скриптов, создающих чрезмерное количество запросов (Flood), даже если они технически не являются DDoS.
- агрессивное сканирование портов

Использование эксплойтов

- Применение готовых или самостоятельно собранных эксплойтов (в том числе для подтверждения уязвимостей), особенно если они затрагивают сторонние библиотеки,

ядро ОС, гипервизоры или сетевую инфраструктуру Cloud.ru.

Сетевые манипуляции

- ARP-spoofing, DNS-poisoning, IP- или MAC-подмены в пределах виртуальной сети;
- Проведение атак типа «Man-in-the-Middle» (MitM) на любые ресурсы, кроме принадлежащих клиенту.

Перехват и анализ чужого трафика

- Любые действия по анализу сетевого трафика, который не является частью принадлежащих клиенту ресурсов (например, перехват пакетов в L2-сетях общего пользования).

Использование нестабильных или экспериментальных инструментов

- Применение инструментов, не прошедших предварительное тестирование в безопасной среде;
- Запуск ПО с неизвестным или нестабильным поведением в продуктивной среде.

Изменение или удаление данных

- Удаление, модификация или перезапись данных (включая журналов, конфигураций и метаданных), за исключением ситуаций, прямо предусмотренных тестовым сценарием и согласованных с Cloud.ru.
- Выход за пределы выделенной клиенту инфраструктуры (контейнер/VM breakout);
- Доступ к данным или системам других клиентов;

Заключительные положения

Компания оставляет за собой право вносить изменения в настоящую Политику в одностороннем порядке с предварительным уведомлением клиентов.

Все споры и разногласия, возникающие в связи с реализацией настоящей Политики, разрешаются путём переговоров, а при необходимости – в порядке, установленном законодательством.

Порядок пересмотра Политики

Настоящая Политика действует до момента ее пересмотра или отмены.
Общее руководство и контроль исполнения требований настоящей Политики возложены на руководителя направления Run облачной платформы.
Пересмотр положений настоящей Политики проводится не реже, чем одного раза в 3 года, а также:

- при изменении используемых в Компании технологий работы Компании;
- при изменении Политики КБ Компании;
- по фактам возникновения инцидентов КБ, выявления уязвимостей;
- по решению руководства Компании.

Ответственность за поддержание Политики в актуальном состоянии возложена на руководителя направления Run облачной платформы.

ПРИЛОЖЕНИЕ 1

Перечень ссылочных документов

1. Политика кибербезопасности ООО «Облачные технологии», утвержденная приказом от 24.09.2021 № П-8.512.
2. Регламент по выводу сервисов на внешний контур, утвержденный приказом от 21.04.2023 № П-8.768.
3. Регламент управления безопасной разработкой программного обеспечения, утвержденный приказом от 14.11.2022 № П-9.694.
4. Руководство по организации процесса управления уязвимостями в органе (организации), утвержден ФСТЭК России 17.05.2023г.