GIS DAYS 2021

Сильные и слабые стороны облачного подхода

Ильин Кирилл
CISO
SberAuto

GIS DAYS

Главные тенденции облачных вычислений 2021

Cloud AI

Orchestration Supremacy

VPC

Improving SaaS AI & ML

Containerization by Industry Giants

Security as a service

Multi-Cloud to Omni-Cloud

Cloud-Native app

Blockchain in Cloud

Преимущества облаков для стартапов

ОБЛАЧНАЯ СТРАТЕГИЯ КАК ПРЕИМУЩЕСТВО ДЛЯ СТАРТАПА

VPC
Virtual Private Cloud

docker

Office 365

G Suite

GitLab

Jira

Confluence

IT-ИНФРАСТРУКТУРА
(IaaS/PaaS/SaaS)

Элементы инфраструктуры, сопровождающие, бизнес-процессы на разных этапах жизненного цикла (от разработки до промышленной эксплуатации)


Infra as Code


Git repository


Container Registry


Container Instances


Kubernetes Services

Инфраструктура как код

Система контроля версий

Реестр артефактов

Контейнеры

Среда оркестрации

Объекты защиты

ОБЛАЧНАЯ СТРАТЕГИЯ КАК ПРЕИМУЩЕСТВО ДЛЯ СТАРТАПА

Внедрение практик DevOps

- Получили ряд дополнительных преимуществ, таких как повышенная гибкость, скорость и снижение затрат в разработке.

Снижение затрат

- Внедрнение концепции Cloud-Native
- использование микросерверной инфраструктуры

Снижение time to market

- DevOps позволил разрабатывать бизнес-приложения в гораздо более короткие сроки.
- Автоматизация процессов разработки, тестирования и развертывания.

Динамическое выделение ИТ-ресурсов

- Управление инфраструктурой как кодом.
- Непрерывный мониторинг производительности приложений и состояния инфраструктуры.

Повышение гибкости в разработке

- Согласование процессов разработки и поставки ПО с эксплуатацией.
- Непрерывное тестирование качества приложений.
- Гибкий процесс управления изменениями.

Обратная сторона медали

- Увеличение количества уязвимостей
- Увеличение поверхности атаки
- Нетипичные угрозы

Темная сторона облака

Риски облаков

Риск провайдера Cloud

- Данные нельзя потрогать
- Общие ресурсы
- Появляются договорные ограничения/SLA/соглашения о КБ
- Ограничения со стороны провайдера (можно сделать только то что разрешает провайдер)
- Непонятен уровень защищенности и вовлеченности провайдера в процессы КБ

Непривычный IaaS

- Программно-определяемое всё
- Не традиционные средства ЗИ
- Высокая сложность и динамичность
- Высокие риски неправильной настройки
- Требует DevSecOps и автоматизации
- Требует понимания специфичных угроз для сред оркестрации и контейнеризации

Проблемный PaaS

- Меньшая гибкость PaaS
- Меньшая степень контроля PaaS
- Ограничение функционала теми возможностями, которые дает оператор сервиса
- Риски безопасности

Партизанский SaaS

- Низкая прозрачность
- Нет контроля за платформой из коробки
- Высокие риски неправильной настройки доступа
- Отсутствие контроля за потоками данных привычный DLP не работает
- Не везде есть возможность классификации данных

Угрозы облаков

Угрозы облаков

1. Утечки данных
2. Неверная конфигурация и недостаточный контроль изменений
3. Отсутствие паттерн безопасной архитектуры и стратегии облачной безопасности.
4. Недостаточная уровень контроля управлением идентификацией, учетными данными, доступом и ключами
5. Взлом аккаунта
6. Внутренние угрозы – угрозы утечки информации
7. Небезопасные интерфейсы взаимодействия и API
8. Непрозрачность использования облачных сервисов - Shadow IT
9. Злоупотребление и неправомерное использование облачных сервисов

Misconfiguration и недостаточный контроль за изменениями

Причины возникновения инцидентов:

- Незащищенные элементы хранения данных или контейнеры
- Чрезмерные разрешения
- Учетные данные по умолчанию и параметры конфигурации оставлены без изменений
- Стандартные средства управления безопасностью отключены

Влияние на бизнес

Влияние неверно настроенного элемента облачного сервиса на бизнес может быть серьезным в зависимости от характера неправильной конфигурации и того, насколько быстро она обнаруживается и устраняется. Наиболее частый эффект - это **раскрытие данных**, хранящихся в облачных репозиториях и ФИР.

Ответственность

- ✓ Владелец услуги
- ✗ Поставщик облачных услуг
- ✗ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✗ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✗ Elevation of Privilege

Отсутствие паттерн безопасной архитектуры облака и стратегии ее развития

Причины возникновения инцидентов:

Одна из самых больших проблем во время перехода в облака - реализация соответствующей архитектуры безопасности, способной противостоять современным кибератакам и угрозам, характерным для облачной инфраструктуры.

Влияние на бизнес

Независимо от размера предприятия, правильная архитектура и стратегия безопасности являются необходимыми элементами для безопасного перемещения, развертывания и работы в облаке.

Успешные кибератаки могут иметь серьезные последствия для бизнеса, включая финансовые потери, репутационный ущерб, юридические последствия и штрафы.

Ответственность

- ✓ Владелец услуги
- ✗ Поставщик облачных услуг
- ✗ Оба

Сервис модель

- ✗ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✓ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✓ Elevation of Privilege

Недостаточный уровень контроля управления идентификацией, учетными данными, доступом и управлением ключами

Причины возникновения инцидентов:

- Неадекватная защита учетных данных
- Отсутствие регулярной автоматической ротации криптографических ключей, паролей и сертификатов
- Отсутствие масштабируемых систем управления идентификацией, учетными данными и доступом.
- Невозможность использования многофакторной аутентификации.
- Отсутствие надежных паролей.

Влияние на бизнес

Злоумышленники, маскирующиеся под законных пользователей, администраторов или разработчиков, могут:

- Читать, изменять и удалять данные
- Получить доступ к управлению и изменению инфраструктурой
- Перехватывать данные
- Релизить вредоносное программное обеспечение, под видом легитимного.

Ответственность

- ✓ Владелец услуги
- ✗ Поставщик облачных услуг
- ✗ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✗ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✗ Elevation of Privilege

Взлом аккаунта

Влияние на бизнес

Захват учетной записи подразумевает полный доступ: контроль над учетной записью, ее службами и данными внутри.

В таком сценарии бизнес-логика, функции, данные и приложения, зависящие от учетной записи, подвергаются риску.

Последствия подверженности риску угона аккаунта имеют очень серьезное влияние на бизнес.

В большинстве случаев угона аккаунта имели место значительные сбои в работе и остановке бизнес-процессов, включая примеры полного уничтожения активов и данных организации.

Последствия кражи аккаунта включают риск утечки данных, который приводит к репутационному ущербу, снижению стоимости бренда, юридической ответственности, раскрытию персональных данных, конфиденциальной и служебной информации.

Ответственность

- Владелец услуги
- Поставщик облачных услуг
- Оба

Сервис модель

- Software as a service (SaaS)
- Platform as a service (PaaS)
- Infrastructure as a service (IaaS)

Угрозы

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Риск утечки

Влияние на бизнес

Внутренние угрозы могут привести к потере конфиденциальной информации и интеллектуальной собственности. Простои системы, связанные с атаками, могут негативно сказаться на производительности компании. Кроме того, потеря данных или другой вред клиентам могут снизить доверие к услугам компании.

Работа с инцидентами внутренней безопасности включает локализацию, устранение последствий, реагирование на инциденты, расследование, анализ после инцидентов, эскалацию, мониторинг и наблюдение. Эти действия могут значительно увеличить рабочую нагрузку компании и увеличить бюджет безопасности.

Ответственность

- ✓ Владелец услуги
- ✗ Поставщик облачных услуг
- ✗ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✓ Spoofing Identity
- ✓ Tampering with Data
- ✗ Repudiation
- ✓ Information Disclosure
- ✗ Denial of Service
- ✓ Elevation of Privilege

Небезопасные интерфейсы интеграции и API

Влияние на бизнес

Несмотря на то что большинство провайдеров стремятся обеспечить, интеграцию безопасности в их модели сервисов, для потребителей этих сервисов критически важно понимать последствия безопасности, связанные с использованием, управлением, оркестровкой и мониторингом облачных сервисов.

Использование не безопасно настроенных интерфейсов и API ставит организации перед множеством проблем, связанных с конфиденциальностью, целостностью, доступностью и невозможностью отказа от совершенного действия.

Ответственность

- ✗ Владелец услуги
- ✗ Поставщик облачных услуг
- ✓ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✗ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✓ Elevation of Privilege

Непрозрачность использования облака

Влияние на бизнес

• Отсутствие управления: когда сотрудники не знакомы или не обучены надлежащему контролю доступа и управления в облачных сервисах, часто можно увидеть конфиденциальные корпоративные данные, размещенные в общем доступе, без учета требований защиты от НСД.

• Неправильно настроенные функции безопасности:
когда сотрудник неправильно настраивает облачный сервис, и он может стать доступным не только для компании, но и для злоумышленника, который в свою очередь может внедрить в сервисы вредоносные программы, бот-сети, вредоносное ПО для майнинга криптовалют и многое другое, что подставит под угрозу контейнеры и среду оркестрации.

Ответственность

- ✗ Владелец услуги
- ✗ Поставщик облачных услуг
- ✓ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✓ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✓ Elevation of Privilege

Злоупотребление и неправомерное использование облачными сервисами

Примеры злоупотребления или неправомерного использования облачными сервисами:

- Запуск DDoS-атак.
- Спам по электронной почте и фишинговые кампании.
- «Майнинг» цифровой валюты.
- Крупномасштабное автоматизированное мошенничество с кликами.
- Атаки методом перебора украденных баз учетных данных.
- Размещение вредоносного или пиратского контента.

Влияние на бизнес

Если злоумышленник скомпрометировал уровень управления облачной инфраструктурой или CI/CD, то он может использовать облачную инфраструктуру в незаконных целях таких как добыча криптовалюты или в качестве альтернативы злоумышленники также могут использовать облако для хранения и распространения вредоносных программ или фишинговых атак.

Ответственность

- ✗ Владелец услуги
- ✗ Поставщик облачных услуг
- ✓ Оба

Сервис модель

- ✓ Software as a service (SaaS)
- ✓ Platform as a service (PaaS)
- ✓ Infrastructure as a service (IaaS)

Угрозы

- ✓ Spoofing Identity
- ✓ Tampering with Data
- ✓ Repudiation
- ✓ Information Disclosure
- ✓ Denial of Service
- ✓ Elevation of Privilege

Тенденции в безопасности облаков

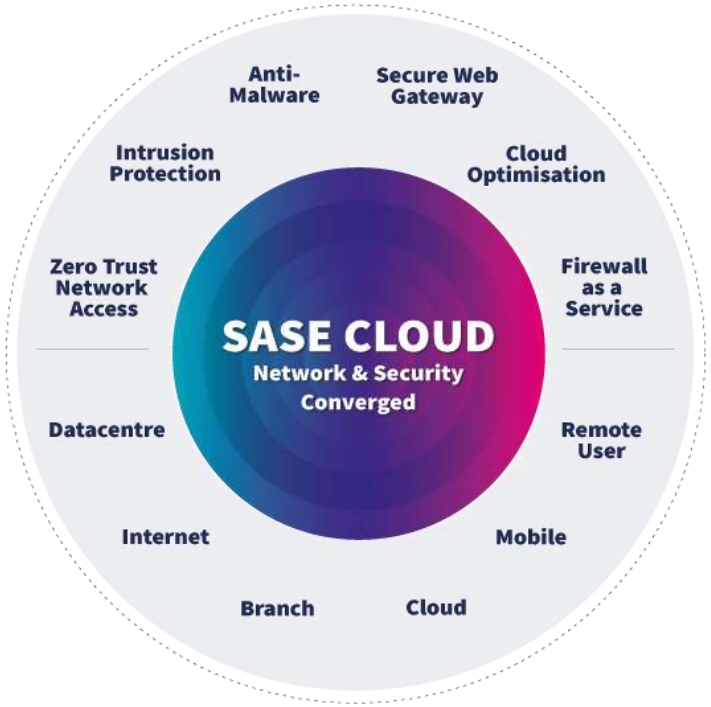
GIS DAYS

Главные тенденции облачной безопасности в 2021

MITRE | ATT&CK®

MITRE | Shield

MITRE | Engage



cloud security alliance℠