вым окнам процесс взаимодействия с пользователем становится более гибким.

Таким образом, при разработке сайта очень важным является создание макета. Существует множество графических редакторов, однако Adobe Illustrator имеет широкий набор инструментов для создания, а также редактирования будущих макетов. Помимо этого есть возможность использовать различные алгоритмы, чтоявляется огромным достоинством Adobe Illustrator среди своих конкурентов.

УДК 004.056.53

Студ. А.А. Цагойко
Науч. рук. преп.-стаж. А.Д. Томко
(кафедра информационных систем и технологий, БГТУ)

ОБЛАЧНЫЕ СЕРВИСЫ: АТАКИ И ЗАЩИТА

Популярность облачных технологий стремительно растет с каждым годом. Невольно этому поспособствовал и пандемический кризис, ставший настоящим стресс-тестом для экономики. Многие компании получили значительные плюсы от перемещения своей инфраструктуры в облако, сумев не только безболезненно пережить 2020 г., но и нарастить объем услуг и выручки. Однако стремительный рост в определенной степени нивелируется наличием множества незащищенных или небезопасно сконфигурированных сервисов.

94% организаций в различной степени обеспокоены безопасностью облака. Согласно проведенному опросу на 2020 год, самые большие угрозы безопасности, с которыми сталкиваются общедоступные облака, это: неправильная конфигурация сервиса (68 %), несанкционированный доступ (58 %), небезопасный интерфейс (52 %), раскрытие аутентификационных данных (50 %).

Утечке данных в облаке в связи с неправильной конфигурацией параметров безопасности способствует несколько факторов. Облачная инфраструктура спроектирована таким образом, чтобы использование и обмен данными не вызывали затруднений. Это приводит к тому, что заказчик не всегда может обеспечить доступ только для уполномоченных сторон. Кроме того, организации, использующие облачную инфраструктуру, не имеют полной видимости и контроля над своей инфраструктурой, а это означает, что необходимо полагаться на меры безопасности, предоставляемые поставщиком облачных услуг.

В отличие от локальной, облачная инфраструктура находится за пределами сети организации и напрямую доступна из Интернета. Это упрощает злоумышленнику несанкционированный доступ к облачным

ресурсам компании при наличии неправильно настроенной политики безопасности или полученных учётных данных.

Взлом учетной записи – одна из наиболее серьезных проблем облачной безопасности, поскольку заказчик все больше полагаются на облачную инфраструктуру и приложения для выполнения основных бизнес-функций. Злоумышленник с учетными данными сотрудника может получить доступ к конфиденциальным данным или функциям, а скомпрометированные учетные данные клиента предоставляют полный контроль над их учетной записью в Интернете. Кроме того, в облаке организациям часто не хватает возможности выявлять эти угрозы и реагировать на них так же эффективно, как и в локальной инфраструктуре.

Следует понимать, что облачная безопасность – это ответственность, которая лежит не только на поставщике услуг, но и на заказчике. Модель общей ответственности по обеспечению безопасности делится на три категории:

– обязанности, которые всегда лежат на провайдере. К ним относятся защита самой инфраструктуры, доступ, установка исправлений и настройка физических хостов и физической сети, в которой выполняются вычислительные экземпляры и размещаются ресурсы и хранилище;

– обязанности, которые всегда лежат на клиенте, включающие в себя управление пользователями и их привилегиями доступа, защиту облачных учётных записей от несанкционированного доступа, шифрование и защиту облачных информационных активов;

– обязанности, которые варьируются в зависимости от модели обслуживания (IaaS, SaaS, PaaS).

Наиболее эффективные способы защиты в области облачной безопасности:

1. Шифрование данных. Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в ЦОД, а также в случаи отсутствия необходимости, безвозвратно удалять.

2.Защита данных при передаче. Зашифрованные данные при доступны только аутентифицированным пользователям. Данные не получится прочитать или сделать изменения, даже в случаи доступа через ненадежные узлы.

3.Аутентификация. 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 и SAML

4. Изоляция пользователей. Использование индивидуальной виртуальной машины и виртуальную сеть. Виртуальные сети должны быть развернуты с применением таких технологий, как VPN, VLAN и VPLS. Часто провайдеры изолируют данные пользователей друг от друга за счет изменения данных кода в единой программной среде. Данный подход имеет риски, связанные с опасностью найти дыру в нестандартном коде, позволяющему получить доступ к данным. В случаи возможной ошибки в коде пользователь может получить данные другого.

Фундаментальный и многосторонний анализ рисков для информационной безопасности является неотъемлемой предпосылкой разработки и сопровождения успешных и эффективных мер по защите информации в условиях облачных вычислений.

Несмотря на все достоинства облачных вычислений, на сегодняшний день потребителям необходимо взвешенно подходить к их внедрению, органично сочетать традиционные (локальные) и облачные инфраструктуры в организации вычислительного процесса.

ЛИТЕРАТУРА

1. Checkpoint [Электронный ресурс] – 2021. – Режим доступа: https://www.check-point.com/cyberhub/cloudsecurity/whatiscloudsecurity/topcloudsecurityissuesthreatsandconcerns/. – Дата доступа: 29.03.2021.

2. Phoenixnap [Электронный ресурс] – 2021. – Режим доступа: https://phoe-nixnap.com/blog/whatiscloudsecurity. – Дата доступа: 29.03.2021.

3. Habr [Электронный ресурс] – 2021. – Режим доступа:https://habr.com/ru-/company/cloud4y/blog/500866/. – Дата доступа: 29.03.2021.

УДК 004.056.53

Студ. Д.И. Леонов
Науч. рук. преп.-стаж. А.Д. Томко
(кафедра информационных систем и технологий, БГТУ)

О РАССТАНОВКЕ СИЛ В SECURITY-СООБЩЕСТВЕ И О КАРТЕ СРЕДСТВ САМОЗАЩИТЫ ЯДРА LINUX

Чего мы ждем от современной операционной системы. Без сомнений – это удобность в использовании, быстродействие и, конечно же, одним из главных критериев является безопасность. Безопасность – это то, что обеспечивает нам защиту от вирусов, комфортное пребы-