Федченко А.С., Бирих Э.В. Безопасность механизмов работы гипервизора // Международный журнал информационных технологий и энергоэффективности.– 2025. – Т. 10 № 2(52) с. 44–54

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.45

БЕЗОПАСНОСТЬ МЕХАНИЗМОВ РАБОТЫ ГИПЕРВИЗОРА

[1]Федченко А.С., Бирих Э.В.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [1]vishnya.fas@gmail.com

В статье представлена обзорная информация о принципах устройства и механизмах работы гипервизоров, их роли в современной ИТ-инфраструктуре и основных угрозах, связанных с виртуализацией. Раскрываются аппаратные и программные аспекты безопасности (изоляция виртуальных машин, контроль привилегий, сегментация сети, мониторинг событий), а также анализируются наиболее распространённые векторы атак, связанные с «побегом» из ВМ и прямым взломом гипервизора. Отдельное внимание уделено практическим рекомендациям по защите виртуализированной среды.

Ключевые слова: Виртуализация, гипервизор, информационная безопасность, управление привилегиями, тестирование на проникновение, аппаратная виртуализация, критические системы.

SECURITY OF THE HYPERVISOR'S MECHANISMS

[1]Fedchenko A.S., Wirrich, E.V.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [1]vishnya.fas@gmail.com

The article provides an overview of the principles of hypervisor design and operation mechanisms, their role in modern IT infrastructure and the main threats associated with virtualisation. Hardware and software security aspects (virtual machine isolation, privilege control, network segmentation, event monitoring) are disclosed, and the most common attack vectors related to VM 'escape' and direct hypervisor hacking are analysed. Special attention is paid to practical recommendations for protecting virtualised environments.

Keywords: Virtualization, hypervisor, information security, privilege management, penetration testing, hardware-based virtualization, critical systems.

Введение

Гипервизор (или виртуальный монитор машин) — это программный или программно-аппаратный слой, который обеспечивает создание и управление виртуальными машинами (ВМ). Гипервизор «обманывает» операционные системы, которые работают внутри виртуальных машин, заставляя их считать, что они используют реальную физическую инфраструктуру. При этом одна физическая машина способна одновременно запускать несколько ВМ с разными операционными системами и конфигурациями.

В своей работе гипервизор отводит каждой виртуальной машине долю ресурсов (процессор, память, диски, сетевые интерфейсы и т.д.) и изолирует их друг от друга. Если бы не гипервизор, такое раздельное использование одних и тех же «железных» ресурсов было бы невозможно или крайне затруднительно.

Сегодня виртуализация стала стандартным инструментом в арсенале любой крупной организации: от банковского сектора до государственных структур и облачных провайдеров. Гипервизоры играют фундаментальную роль в центрах обработки данных (ЦОД), позволяя оптимизировать нагрузку, повышать гибкость инфраструктуры и экономить на физических серверах.

Однако широкое распространение виртуализации выводит на передний план вопросы информационной безопасности. Если в традиционной (не виртуализированной) среде мы имеем дело с «один сервер — одна ОС», то при виртуализации за тем же сервером могут работать десятки или даже сотни виртуальных машин. В случае удачной атаки на гипервизор злоумышленник может получить практически полный контроль над всеми виртуальными машинами, запущенными на данном узле, а это значительно повышает риск конфиденциальных утечек, саботажа и других критических последствий.

Кроме того, растёт важность корректного управления доступом и ролями (кто может конфигурировать гипервизор, запускать/останавливать ВМ, вносить изменения в сетевые настройки и т.д.). Ошибки конфигурации, слабые пароли и устаревшее программное обеспечение становятся потенциальными «дырами» в безопасности, поэтому грамотная стратегия защиты гипервизора — обязательное требование для любой организации, стремящейся снизить киберриски.

Таким образом, изучение принципов работы гипервизоров — не только технически интересная, но и практически необходимая задача для ИБ-специалистов. Знание механизмов виртуализации помогает глубже понимать, на каких уровнях и каким образом могут быть скомпрометированы системы, а также как эффективно противостоять атакам.

Основные типы гипервизоров

Среди современных решений в области виртуализации выделяют несколько ключевых подходов, наиболее заметными из которых являются гипервизоры, работающие напрямую с аппаратной средой (Type-1), и гипервизоры, устанавливаемые поверх существующей операционной системы (Type-2). В первом случае программный компонент взаимодействует с «чистым железом» без участия промежуточного хост-ОС. Такая конфигурация обеспечивает более высокий уровень производительности, поскольку гипервизор напрямую распределяет процессорные, сетевые и дисковые ресурсы между виртуальными машинами. Именно на этой архитектуре основаны решения корпоративного класса, среди которых часто упоминают VMware ESXi, Hyper-V от Microsoft и Xen, широко используемый в облачных средах. Отсутствие полноценной хост-операционной системы снижает вероятность возникновения уязвимостей, связанных с лишними компонентами, однако требует строгого соблюдения процедур обновления и мониторинга, поскольку компрометация самого гипервизора ставит под угрозу все запущенные на нём виртуальные машины.

Подход, при котором гипервизор размещается поверх уже работающей операционной системы, не нуждается в прямом доступе к аппаратному обеспечению. Этот тип виртуализации удобен для небольших сред, лабораторных стендов и повседневных нужд разработчиков. Продукты, такие как VMware Workstation, Oracle VM VirtualBox и Parallels Desktop, функционируют в режиме «приложений», обращающихся к ресурсам ЦП, памяти и сетевых интерфейсов через механизм хост-ОС. С одной стороны, подобное решение упрощает установку и интеграцию в существующую инфраструктуру. С другой стороны, уровень

безопасности во многом зависит от состояния операционной системы хоста, её обновлённости и корректной настройки. Любая уязвимость в хост-ОС может автоматически стать точкой проникновения в виртуальные машины, поскольку гипервизор размещён не в привилегированном, а в пользовательском режиме [1].

Отдельного внимания заслуживает контейнерная виртуализация, которую обычно рассматривают как альтернативный или дополнительный уровень абстракции, позволяющий приложению совместно использовать ядро одной операционной системы. При таком подходе гостевым средам не требуется собственное виртуализированное «железо»: все контейнеры работают на базе общего ядра, что существенно снижает вычислительные накладные расходы и ускоряет развёртывание сервисов. Наиболее распространёнными примерами выступают Docker, LXC и Podman, где каждая изолированная среда владеет собственным пространством процессов, файловой системой и сетевой конфигурацией. Однако общая природа ядра порождает дополнительные риски, связанные с тем, что потенциальная уязвимость в ядре может затронуть все контейнеры одновременно. Поэтому грамотная конфигурация, регулярные обновления и соблюдение стандартов безопасности при подготовке контейнерных образов имеют критическое значение.

Таким образом, выбор технологии виртуализации во многом определяется характером нагрузки, требованиями к производительности и от уровня защищённости, необходимого для работы с персональными данными. Например, для ИСПДн предпочтительнее Type-1 гипервизоры, так как они предоставляют более высокий уровень изоляции [2]. Hosted (Type-2) варианты удобны для тестирования, обучения и случаев, когда не требуется создавать дополнительные уровни безопасности на «чистом железе». Контейнеры, в свою очередь, обеспечивают максимальную гибкость и масштабируемость, но требуют особого подхода к вопросам защиты. Все эти аспекты подчёркивают важность правильного выбора гипервизора и систематических мер безопасности при проектировании и эксплуатации современных вычислительных сред.

Архитектура и базовые механизмы работы гипервизора

Современные процессоры (Intel, AMD) поддерживают многоуровневую модель привилегий (rings), где Ring 0 обычно зарезервирован для ядра операционной системы, а Ring 3 — для пользовательских приложений. При этом для гипервизоров аппаратно предусмотрен отдельный, более привилегированный уровень (иногда его условно называют Ring -1). Именно этот уровень и позволяет гипервизору перехватывать операции ОС-гостя и перенаправлять их на реальные аппаратные ресурсы.

- Ring -1 (Hypervisor mode). Самый привилегированный уровень, в котором может выполняться код гипервизора.
- Ring 0 (Kernel mode). Уровень работы традиционного ядра операционной системы (гость, хост).
- Ring 3 (User mode). Уровень обычных пользовательских процессов.

Важнейшим аспектом функционирования гипервизора становится виртуализация вычислительных ресурсов, включающая в себя несколько ключевых компонентов.

Одним из них выступает процессорная виртуализация, основанная на использовании технологий Intel VT-x и AMD-V. Эти аппаратные расширения дают возможность гостевой ОС

выполнять большинство инструкций напрямую, с минимальным вмешательством гипервизора, который вмешивается только в «опасные» или привилегированные операции.

Параллельно с этим функционирует механизм виртуализации памяти, отвечающий за раздельное адресное пространство для каждой виртуальной машины. Наиболее современным решением считается использование Extended (или Nested) Page Tables, позволяющих процессору самостоятельно поддерживать два набора таблиц страниц — для гостя и для гипервизора. Такое разделение даёт возможность эффективно изолировать области памяти разных виртуальных машин и снижает накладные расходы за счёт уменьшения количества переключений контекста [3].

Специфика взаимодействия с периферийными устройствами и системами ввода-вывода требует дополнительного внимания к виртуализации I/O. В одних случаях гипервизор эмулирует устройства для гостевой системы, предоставляя ей универсальные драйверы, которые «маскируют» физический адаптер или контроллер. В других случаях применяется паравиртуализация, когда внутри гостевой ОС устанавливаются специальные драйверы, способные взаимодействовать с гипервизором напрямую. Такой подход повышает производительность и снижает число дорогостоящих эмулируемых операций. Иногда, если требуется особенно высокая пропускная способность, оборудование пробрасывается напрямую в гостевую систему (passthrough), что фактически даёт виртуальной машине эксклюзивный доступ к конкретному устройству. Однако подобная схема сокращает гибкость инфраструктуры и требует более строгого контроля безопасности.

Вся совокупность механизмов виртуализации дополняется процедурами управления жизненным циклом виртуальных машин. Гипервизор выделяет ресурсы под каждую виртуальную машину, загружает гостевую операционную систему и контролирует ряд важных процессов: от инициализации и планирования ресурсов до миграции работающих ВМ между разными физическими узлами без простоя. Такой «гибридный» контроль над программно-аппаратной конфигурацией позволяет динамически изменять число виртуальных процессоров, распределять объём оперативной памяти, оптимизировать сетевые настройки и даже отслеживать состояние гостевых ОС. Кроме того, реализованная в большинстве корпоративных платформ функция «живой» миграции даёт возможность переносить ВМ на другие хосты практически без перерыва в обслуживании, что особенно важно для центров обработки данных, требующих непрерывной доступности.

Все перечисленные механизмы формируют технологическую основу гипервизора, которая удерживает баланс между производительностью, гибкостью и безопасностью. Поддержка нескольких уровней привилегий, тонкая настройка распределения памяти и паравиртуализация делают возможным одновременный запуск множества гостевых систем без критических потерь в скорости работы. При этом чёткая аппаратно-программная сегментация ресурсов обеспечивает надёжную изоляцию, необходимую для противодействия попыткам несанкционированного вмешательства или распространения сбоев, инициируемых внутри одной виртуальной машины.

Механизмы защиты и обеспечение безопасности

Одна из ключевых функций гипервизора — обеспечение строгой изоляции виртуальных машин друг от друга. Это достигается за счёт аппаратных (Intel VT-x, AMD-V) и программных (EPT/NPT, Shadow Page Tables) механизмов, которые не позволяют одной ВМ напрямую

обращаться к памяти или устройствам другой ВМ. Изоляция включает в себя несколько аспектов:

- Память. Каждая гостевая ОС видит только «своё» адресное пространство; гипервизор блокирует любые попытки прямого доступа к чужим участкам.
- Сеть. Сетевая изоляция может осуществляться с помощью виртуальных свитчей, VLAN, виртуальных маршрутизаторов и firewall. Это позволяет создавать полноценные сегментированные среды внутри одного физического узла.
- Устройства I/O. Физические устройства могут быть «проброшены» напрямую в конкретную ВМ, или эмулироваться и паравиртуализироваться. Правильная конфигурация механизмов ввода-вывода снижает риск «утечки» данных между виртуальными машинами[4].

Неотъемлемым элементом защиты является также контроль привилегий, который реализуется через сложную систему аутентификации и авторизации внутри гипервизора. Чтобы гарантировать безопасность этого уровня, во всех крупных системах виртуализации предусмотрена разграниченная модель управления, в рамках которой права пользователей чётко соответствуют выполняемым функциям.

Такой подход наиболее эффективен при условии задействования корпоративных систем аутентификации (LDAP, Kerberos, Active Directory), где политики безопасности, включающие многофакторную аутентификацию, повышают надёжность доступа к административным интерфейсам. Кроме того, многочисленные исследования показывают, что ошибки конфигурации и недостаток внимания к механизмам разграничения прав часто становятся первопричиной компрометации гипервизора, что подчёркивает важность формального контроля и регулярного аудита учётных записей[5].

Без эффективного мониторинга и аудита невозможно оперативно выявлять попытки несанкционированного вмешательства в виртуализированную среду. Логирование в гипервизорах обычно охватывает сведения о запуске, остановке, миграции и изменениях параметров виртуальных машин, а также о действиях администраторов и системных сбоях. Централизованный сбор этих данных с последующим анализом в SIEM-платформах позволяет не только обнаружить аномалии в поведении отдельных систем, но и коррелировать их с событиями на сетевом и прикладном уровнях. Существенным преимуществом современной виртуализации является возможность внедрять виртуальные модули обнаружения вторжений (vIDS) непосредственно в программные свитчи, чтобы контролировать трафик между виртуальными машинами до того, как он выйдет на физическую сеть или будет маршрутизирован вовне.

Наконец, для защиты целостности гипервизора необходимо внедрение аппаратных и программных мер, препятствующих его подмене или несанкционированной модификации.

- Применение модуля доверенной платформы (TPM) и технологии безопасной загрузки (Secure Boot) помогает удостовериться, что гипервизор не был модифицирован или подменён вредоносным ПО.
- Обновление и патчинг. Уязвимости в гипервизорах регулярно обнаруживаются и закрываются производителями. Игнорирование обновлений создаёт прямую угрозу «пробоя» всей виртуализированной среды.
- Минимизация «поверхности атаки». Не устанавливать лишние модули и плагины, не активировать ненужные сервисы (веб-интерфейсы, API, порты). Чем меньше

функциональных элементов доступно в гипервизоре, тем сложнее злоумышленникам найти уязвимость.

Типовые угрозы и уязвимости гипервизоров

Среди наиболее опасных сценариев, связанных с гипервизорами, одним из самых известных является так называемый «побег» из виртуальной машины, при котором злоумышленник, действуя из гостевой операционной системы, добивается выполнения кода на уровне гипервизора или хост-ОС. Такая возможность, именуемая VM Escape, подрывает фундаментальную изоляцию между виртуальными машинами и ставит под угрозу безопасность всей виртуализированной среды. Во многих случаях она реализуется благодаря уязвимостям в модулях эмуляции устройств (например, сетевых адаптеров или USB-контроллеров), ошибкам в драйверах паравиртуализации или неверным настройкам режима пассконтроля (passthrough). Данные факторы открывают путь для атакующего не только к ресурсам скомпрометированной ВМ, но и к соседним окружениям, а также к самому гипервизору. В целях предотвращения подобных инцидентов применяются аппаратные (VT-x, AMD-V) и программные (EPT/NPT) механизмы перехвата опасных инструкций, равно как и дополнительные технологии сегментации и контроля привилегий.

Не меньшую угрозу представляет возможность прямой атаки на гипервизор, которая подразумевает поиск и эксплуатацию уязвимостей в самом программном коде платформы виртуализации или её управляющих компонентах. Оказавшись в привилегированном режиме (Ring -1), злоумышленник получает полный контроль над всеми запущенными виртуальными машинами, что ведёт к тотальному срыву мер информационной безопасности. Чаще всего проникновение осуществляется через веб-консоли управления или автоматизированные интерфейсы (API), открытые для внешнего мира. Ситуацию усугубляет загрузка недоверенных образов виртуальных машин, чьи внутренние механизмы могут быть специально сфокусированы на эксплуатации конкретных уязвимостей гипервизора. Надёжную защиту обеспечивает комплексный подход, основанный на строгих политиках доступа к сервисам управления, регулярном патчинге и многофакторной аутентификации для всех привилегированных пользователей.

Ещё одним типом распространённой угрозы следует считать атаки, направленные против соседних виртуальных машин внутри одной физической платформы, то есть так называемые VM-to-VM-атаки. На практике они становятся возможны при наличии единого сегмента виртуальной сети, куда злоумышленник получает доступ, взломав одну из виртуальных машин. В такой ситуации возникает риск перехвата или перенаправления трафика, а также анализа открытых портов и сервисов остальных ВМ. Для снижения вероятности подобных атак рекомендуют внедрять VLAN или VXLAN, задействовать межсетевые экраны (vFirewall), включать системы обнаружения вторжений (vIDS/IPS) и настраивать сетевую политику так, чтобы каждая машина имела собственный, чётко очерченный периметр.

Не стоит забывать и о человеческом факторе, который во многих случаях сводит на нет технологические меры защиты. Администраторы гипервизоров нередко оставляют пароли по умолчанию, злоупотребляют правами с неограниченным доступом или пренебрегают шифрованием административных каналов. Кроме того, отсутствие надлежащих процедур аудита и контроля действий повышает риск инсайдерских угроз, когда сотрудник с высокими

привилегиями умышленно или по неосторожности наносит урон всей виртуализированной инфраструктуре. Чтобы сократить подобные риски, критически важно проводить регулярные обучения персонала, формально закреплять принципы разграничения прав и настаивать на многофакторной аутентификации при работе с любыми управляющими консолями. Соответствующие меры профилактики включают ведение детального журнала действий, непрерывный анализ конфигурационных изменений и внедрение механизма подтверждения особо важных операций несколькими ответственными лицами. Все эти шаги в совокупности образуют прочный каркас защиты, необходимый для противодействия наиболее опасным и распространённым атакам на гипервизоры.

Рекомендации по безопасной работе

Надёжное функционирование виртуализированной среды во многом определяется комплексностью и системностью подхода к её защите. В первую очередь имеет смысл обратить особое внимание на окружение гипервизора: чем меньше сервисов и приложений активно работают на уровне базовой инфраструктуры, тем сложнее злоумышленнику найти точку входа. Минимизация «поверхности атаки» достигается за счёт отключения лишних функций и портов, а также ограничения доступа к любым административным консолям, которые должны быть доступны лишь из доверенных сегментов сети. При этом актуальность устанавливаемого программного обеспечения приобретает критическое значение, поскольку своевременные патчи и регулярные обновления устраняют потенциальные бреши в системе, прежде чем они будут обнаружены и эксплуатированы. Дополнительную надёжность обеспечивает задействование аппаратных компонентов, вроде TPM и технологий безопасной загрузки (Secure Boot), гарантирующих целостность кода гипервизора на самых ранних этапах его функционирования [6].

Не менее важно грамотно сегментировать виртуальную инфраструктуру и разграничивать права доступа, чтобы одна скомпрометированная машина не становилась плацдармом для атаки на весь гипервизор и соседние окружения. Виртуальные машины целесообразно объединять в изолированные сети или VLAN с учётом их роли в корпоративной инфраструктуре и критичности обрабатываемых данных. Такие меры препятствуют горизонтальному проникновению и одновременно упрощают мониторинг трафика. В рамках управления учётными записями целесообразно использовать принцип наименьших привилегий, когда каждый администратор или сервис получает строго оговорённый набор функций. Более того, многофакторная аутентификация становится фактически обязательным требованием для всех полномочий, способных повлиять на состояние гипервизора. Подобная тактика существенно повышает уровень защиты и осложняет задачу потенциальным нарушителям.

Без специализированных инструментов выявить ранние признаки атаки или несогласованные изменения в конфигурации оказывается крайне трудно. Поэтому системы обнаружения вторжений (в том числе виртуальные IDS/IPS, работающие внутри программных свитчей) помогают контролировать внутренний трафик и выявлять аномальное поведение до того, как оно распространится за пределы одной виртуальной машины. Логи гипервизора и гостевых систем, собранные и проанализированные централизованно, дают возможность своевременно отследить необычные действия, а интеграция с SIEM-решениями обеспечивает более широкую корреляцию данных и автоматические уведомления в случае подозрительных

инцидентов. Немаловажную роль играет и шифрование: закрытие административных каналов посредством надёжных криптографических протоколов, равно как и шифрование хранилищ виртуальных дисков, существенно затрудняет попытки перехвата конфиденциальной информации.

Завершая контур безопасности, следует заложить процедуру регулярного аудита и тестирования на проникновение, а также детально прописать план реагирования на инциденты. Периодическая проверка конфигурации гипервизора и виртуальных машин помогает вовремя выявлять неиспользуемые сервисы, неверно настроенные сетевые политики или устаревшие пакеты. Проведение сканирования уязвимостей и пентестов укрепляет уверенность в корректной защите, а также позволяет точнее оценить потенциальный ущерб в случае реальной атаки. При этом заранее продуманный план реагирования с чёткими ролями и процедурами, включающими восстановление из резервных копий, даёт возможность быстро остановить развитие инцидента и минимизировать его влияние на деятельность организации. Если все перечисленные элементы — изоляция, сегментация, контроль доступа, мониторинг, тестирование и планирование аварийного восстановления — последовательно внедрены и регулярно совершенствуются, то виртуализированная среда получает комплексную и многоуровневую систему защиты, способную противостоять современным киберугрозам.

Реальные кейсы и примеры атак

Практика эксплуатации гипервизоров демонстрирует, что даже тщательно спроектированные системы подвержены атакам, иногда приводящим к массовым компрометациям и нанесению значительного ущерба. В ряде случаев преступные группировки фокусировались на уязвимостях в VMware ESXi, применяя шифровальщиков (ransomware) с целью парализовать все виртуальные машины, работающие на одном сервере. Такая тактика позволяла злоумышленникам за считаные часы останавливать ключевые бизнес-процессы и требовать от организаций значительные суммы за расшифровку данных. Многие компании, столкнувшиеся с этой угрозой, констатировали, что несвоевременное обновление гипервизора и слабые пароли в административных консолях стали определяющими факторами, упростившими проведение атак[7].

Схожие инциденты затрагивали Microsoft Hyper-V, где в отдельных версиях были обнаружены уязвимости, допускающие так называемый частичный «побег» из виртуальной машины, когда злоумышленник, действуя из гостевой ОС, мог попытаться выполнить произвольный код на уровне гипервизора. Хотя последующие патчи и программные блокировки снизили вероятность успешной эксплуатации, некоторые предприятия, не позаботившиеся о своевременной установке обновлений, подверглись серьёзным атакам, связанных с несанкционированным доступом к конфиденциальной информации. Подобное развитие событий вновь указывает на ключевую роль регулярного мониторинга и систематического тестирования уязвимостей.

Не меньшую угрозу представляют и уязвимости в гипервизорах Xen, чьи бюллетени безопасности (Xen Security Advisories, XSA) периодически содержат описания критических проблем. К примеру, достаточно известный инцидент произошёл в 2015 году, когда одна из уязвимостей позволяла гостевой ОС некорректно обрабатывать hypercall и потенциально перехватывать управление гипервизором. В результате крупным облачным провайдерам, использующим Xen для виртуализации, пришлось в экстренном порядке устанавливать

обновления и временно перезагружать обширные кластеры, чтобы пресечь возможные атаки на инфраструктуру. Этот случай подчёркивает, что даже широко признанные и тщательно проработанные решения оказываются уязвимы без непрерывного сопровождения и исправления обнаруженных дефектов [8].

Сопоставительный анализ подобных инцидентов позволяет выделить несколько общих черт, свидетельствующих о ключевых факторах успеха взлома. В первую очередь недостаточное внимание уделяется своевременному применению патчей, открывающему «окно возможностей» для атакующих, особенно когда сведения о конкретной уязвимости становятся публичными. Во-вторых, в одной среде виртуализации часто смешиваются машины различного уровня критичности, что даёт злоумышленнику шанс получить начальный доступ через наименее защищённую ВМ и затем двигаться к более ценным целям, сканируя внутреннюю сеть и эскалируя привилегии. Кроме того, во многих организациях отсутствует жёсткий контроль за образами виртуальных машин, в результате чего заражённые шаблоны или неподтверждённые ISO-образы незаметно встраивают вредоносный код прямо на этапе развёртывания инфраструктуры.

Не менее важно учитывать человеческий фактор, нередко проявляющийся в формальном отношении к парольной политике или слишком широких административных правах. Расследования показали, что ряд сотрудников, ответственных за конфигурацию гипервизора, в некоторых случаях применял тривиальные пароли, передававшиеся в незащищённом виде, либо открывал доступ к веб-консолям из общедоступного сегмента Интернета. Вдобавок к этому во время инцидентов не всегда оказывалась подготовлена продуманная схема реагирования, что усиливало негативные последствия для бизнеса. Таким образом, совокупный опыт реальных атак свидетельствует о важности комплексного и непрерывного подхода к информационной безопасности, где технические меры (патчинг, сегментация, мониторинг трафика) должны сочетаться с организационными инструментами (регламенты доступа, обучение персонала, чёткий план действий при обнаружении инцидента). Подобная интеграция даёт возможность своевременно отсеивать уязвимые узлы в виртуализированной среде и эффективно нейтрализовать даже сложные векторы атаки.

Заключение

Возможности виртуализации, обеспечиваемые гипервизорами, прочно закрепились в современном ИТ-ландшафте, поскольку позволяют объединять высокую производительность с гибкостью управления ресурсами. Однако рост значимости гипервизоров одновременно превращает их в приоритетные мишени для атак, что делает комплексные меры безопасности обязательным требованием. Технологии аппаратной поддержки (такие как Intel VT-x или AMD-V) и дополнительные механизмы защиты (включая Secure Boot и TPM) создают мощный фундамент для надёжной изоляции виртуальных машин, но в условиях непрерывно развивающихся угроз этого уже недостаточно. Чтобы обеспечить устойчивость системы, необходимо не только следить за своевременным обновлением гипервизора и его компонентов, но и проводить аудит конфигурации, уделять внимание разграничению прав пользователей и вовлекать механизмы мониторинга и анализа событий.

Таким образом, гипервизоры выступают не просто инструментом виртуализации, а фундаментом, на котором выстраивается вся современная ИТ-инфраструктура. Надёжность этого «фундамента» определяется как аппаратной архитектурой, так и грамотным подбором

организационных мер, мониторинговых решений и методик реагирования на инциденты. Ключевым фактором остаётся непрерывное совершенствование: стремительный характер технологических преобразований предъявляет всё более высокие требования к безопасности, делая профессиональный обмен знаниями и практиками одним из важнейших условий успешной эксплуатации гипервизоров в самых разнообразных сценариях.

Список литературы

1. VMware. Официальная документация [Электронный ресурс]. — Режим доступа: https://docs.vmware.com/en/VMware-vSphere/index.html (дата обращения: 23.12.2024).
2. Бирих, Э. В. К вопросу об аудите персональных данных / Э. В. Бирих, С. С. Ферапонтова // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018) : VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах, Санкт-Петербург, 28 февраля – 01 2018 года / Под редакцией С.В. Бачевского. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2018. – С. 111-114. – EDN UTRRPG
3. Red Hat. Технологии виртуализации (KVM, oVirt) [Электронный ресурс]. — Режим доступа: https://www.redhat.com/ru/technologies/virtualization (дата обращения: 23.12.2024).
4. Xen Project. Официальная документация [Электронный ресурс]. — Режим доступа: https://xenproject.org/developers/documentation/ (дата обращения: 23.12.2024).
5. Microsoft. Документация по Hyper-V [Электронный ресурс]. — Режим доступа: https://learn.microsoft.com/ru-ru/windowsserver/virtualization/hyper-v/hyper-v-technology-overview (дата обращения: 23.12.2024).
6. Souppaya M., Scarfone K. Guidelines for Managing the Security of Mobile Devices in the Enterprise. National Institute of Standards and Technology (NIST), Special Publication 800-124, Rev. 1 [Электронный ресурс]. — Режим доступа: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf (дата обращения: 23.12.2024).
7. VMware. Влияние атак шифровальщиков на инфраструктуру VMware ESXi [Электронный ресурс]. — Режим доступа: https://blogs.vmware.com/security/ (дата обращения: 23.12.2024).
8. Xen Project. Xen Security Advisories (XSA-148) [Электронный ресурс]. — Режим доступа: https://xenproject.org/security-advisories/ (дата обращения: 23.12.2024).

References

1. VMware. Official Documentation [Electronic resource]. — Access mode: https://docs.vmware.com/en/VMware-vSphere/index.html (accessed: 23.12.2024).
2. Birikh, E. V., Ferapontova, S. S. On the Issue of Personal Data Auditing / E. V. Birikh, S. S. Ferapontova // Current Issues of Infotelecommunications in Science and Education (APINO 2018): Proceedings of the VII International Scientific, Technical, and Methodological Conference. 4 Volumes. Saint Petersburg, February 28 – March 01, 2018 / Edited by S. V. Bachevsky. Volume 1. — Saint Petersburg: Saint Petersburg State University of

Telecommunications named after prof. M.A. Bonch-Bruevich, 2018. — P. 111-114. — EDN UTRRPG.

3. Red Hat. Virtualization Technologies (KVM, oVirt) [Electronic resource]. — Access mode: https://www.redhat.com/ru/technologies/virtualization (accessed: 23.12.2024).
4. Xen Project. Official Documentation [Electronic resource]. — Access mode: https://xenproject.org/developers/documentation/ (accessed: 23.12.2024).
5. Microsoft. Hyper-V Documentation [Electronic resource]. — Access mode: https://learn.microsoft.com/ru-ru/windowsserver/virtualization/hyper-v/hyper-v-technology-overview (accessed: 23.12.2024).
6. Souppaya M., Scarfone K. Guidelines for Managing the Security of Mobile Devices in the Enterprise. National Institute of Standards and Technology (NIST), Special Publication 800-124, Rev. 1 [Electronic resource]. — Access mode: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf (accessed: 23.12.2024).
7. VMware. The Impact of Ransomware Attacks on VMware ESXi Infrastructure [Electronic resource]. — Access mode: https://blogs.vmware.com/security/ (accessed: 23.12.2024).
8. Xen Project. Xen Security Advisories (XSA-148) [Electronic resource]. — Access mode: https://xenproject.org/security-advisories/ (accessed: 23.12.2024).