УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ: ЩИТ ОТ КИБЕРУГРОЗ

Н.Ю. Кугрышева[а], студентка гр. 17В41,
Научный руководитель: Воробьев А.В., к.т.н., доц.
Юргинский технологический институт (филиал)
Национального исследовательского Томского политехнического университета
652055, Кемеровская обл. г. Юрга, ул. Ленинградская, 26
E-mail: [а]nyphr4w@tpu.ru

Аннотация: В данной статье представлен обзор основных принципов и практических подходов к организации процесса управления уязвимостями для повышения уровня безопасности современных IT-систем.

Ключевые слова: управление уязвимостями, информационная безопасность.

Abstract: This article provides an overview of the fundamental principles and practical approaches to organizing a vulnerability management process to enhance the security of modern IT systems.

Keywords: vulnerability management, information security (infosec).

Информация всегда была ключевым активом. В наши дни огромные объёмы данных хранятся и передаются в цифровом пространстве. Организации всех размеров полагаются на информационные технологии для ведения бизнеса. И вместе с этим увеличивается количество угроз, способных нанести вред. Поэтому обеспечение защиты информации становится критически важной задачей.

Управление уязвимостями – поиск, анализ и устранение слабых мест в системе (программном обеспечении, аппаратных средствах, сетевых компонентах и даже в процессах организации), которые могут быть использованы злоумышленником для получения несанкционированного доступа.

Успешная атака может не только привести к утечке данных, простоям системы, серьёзным финансовым потерям и нанести ущерб репутации, но и повлечь за собой юридическую ответственность компании.

Существуют различные категории уязвимостей, каждая из которых представляет собой потенциальную угрозу для безопасности информационных систем.

Некоторые уязвимости идентифицируются по своим названиям. Но в большинстве случаев эксперты используют уникальные идентификаторы CVE, которые заносятся в специализированные базы данных, такие как NVD (National Vulnerability Database).

Основные категории:

- Программные уязвимости – недочёты и ошибки в программном коде.

К примеру, переполнение буфера позволяет внедрять вредоносный код, а SQL-инъекции позволяют злоумышленникам обходить защиту и получать доступ к базам данных, изменяя SQL-запросы.

- Сетевые уязвимости – недостаточная защита сетевой инфраструктуры.

Использование простых паролей и устаревших протоколов Wi-Fi делает сеть уязвимой для несанкционированного доступа, перехвата данных и манипулирования трафиком.

- Конфигурационные уязвимости – некорректные настройки систем и приложений.

Открытые и доступные извне интерфейсы могут предоставить неавторизованный доступ к системе. Некорректно настроенные права доступа позволяют злоумышленникам повысить свои привилегии и получить контроль над конфиденциальными данными.

- Аппаратные уязвимости – конструктивные недостатки оборудования.

К примеру, Meltdown и Spectre, позволяющие злоумышленникам извлекать данные из оперативной памяти различных устройств, включая смартфоны, компьютеры и серверы.

- Уязвимости, связанные с процессами и политиками безопасности – недоработки в организационных процедурах, правилах безопасности и обучении персонала.

Использование слабых паролей, отсутствие регулярного резервного копирования данных или недостаточная осведомлённость сотрудников о методах социальной инженерии облегчают злоумышленникам проникновение в систему и компрометацию данных.

Не все уязвимости становятся целью для хакерских атак. Наиболее популярные и многократно используемые из них называют трендовыми.

Некоторые из актуальных уязвимостей на основе данных базы NVD, затрагивающих программное обеспечение и оборудование, используемое в государственных и корпоративных структурах:

- Windows.

Уязвимости CVE-2024-38014 и CVE-2024-38217 предоставляют возможность повышения привилегий локально до уровня SYSTEM в обход механизма защиты Mark of the Web, что позволяет успешно маскировать вредоносные файлы, выдавая их за безопасные.

- Veeam Backup & Replication.

Уязвимость CVE-2024-40711 предоставляет возможность удалённого выполнения кода без необходимости аутентификации, что серьёзно угрожает безопасности сервера и может полностью скомпрометировать всю инфраструктуру.

- VMware vCenter.

Уязвимость CVE-2024-38812 также позволяет неавторизованным лицам удалённо выполнять произвольный код и контролировать сервер vCenter.

- Веб-приложения.

Уязвимости CVE-2024-37383 и CVE-2024-8275 идентифицированы в Roundcube Webmail и плагине The Events Calendar для WordPress. Они открывают доступ к базе данных и позволяют злоумышленникам выполнять JavaScript-код, что ставит под угрозу безопасность учётных записей пользователей.

- Процессоры.

Уязвимости GhostRace и RFDS, затрагивающие архитектуры Intel, AMD и ARM, позволяют извлекать конфиденциальные данные с помощью спекулятивных методов атак.

Этапы управления уязвимостями

Инвентаризация и классификация активов компании.

Составляется исчерпывающий список всех ресурсов компании. Этот список может включать: физические и виртуальные серверы, сетевое оборудование, конечные устройства, системы управления, используемое программное обеспечение и прочее.

После этого активы классифицируются по степени важности. Например, серверы, содержащие базу данных клиентов, требуют более пристального внимания, чем тестовые серверы.

Наконец, за каждым активом закрепляется ответственный сотрудник или команда. Это позволяет оперативно реагировать на возможные инциденты.

Выявление уязвимостей (Сканирование).

Существует два основных способа выявления рисков:

- Автоматическое сканирование – позволяет оперативно обнаружить бреши в системе безопасности, которые уже внесены в списки специализированных баз данных.
- Тестирование на проникновение – имитация реальной кибератаки. Позволяет выявить более сложные уязвимости и потенциально слабые места, которые автоматическое сканирование может пропустить. Это требует больших усилий, но обеспечивает более глубокий анализ.

Оценка проблем безопасности (Приоритизация).

Определяется порядок устранения уязвимостей. При расстановке приоритетов необходимо учитывать лёгкость эксплуатации уязвимости, возможный ущерб и количество затронутых систем. Для оценки рисков используют CVSS и другие источники информации об угрозах. Важно помнить, что эти источники освещают только распространённые уязвимости, поэтому не следует пренебрегать тестированием на проникновение и работой с уязвимостями нулевого дня.

Устранение проблем безопасности.

На данном этапе есть три возможных подхода:

- Полное устранение – установка обновлений программного обеспечения или изменение настроек безопасности.
- Смягчение последствий – отключение уязвимого устройства может стать временной мерой, если нет возможности оперативно устранить угрозу.
- Принятие рисков – определение уязвимости, как некритичной.

Отчётность.

Регистрируется вся информация о проделанной работе: выявленные уязвимости, их описание, выполненные работы по их устранению и текущий статус. Данная документация служит основой для будущих аудитов безопасности.

Специалистам по информационной безопасности ежедневно приходится обрабатывать и приоритезировать большое количество потенциальных угроз. В средних и крупных компаниях только ручная обработка непродуктивна. Для повышения производительности внедряется автоматизация с использованием различных инструментов: от коммерческих продуктов до сервисов управления уязвимостями и open-source решений.

1. Вендорские решения

Предоставляют полный набор инструментов для сканирования, анализа, приоритизации и устранения угроз. Преимуществом таких решений является простота их интеграции и готовность к использованию с минимальными настройками.

На рынке есть российские решения для комплексной защиты: MaxPatrol VM и R-Vision VM.

- MaxPatrol VM от компании Positive Technologies.

Легко настраивается. Поддерживает как активное, так и пассивное сканирование, включая протоколы TCP/UDP. Для доступа к сетям и серверам платформа использует протоколы SNMP, SSH, WMI.

Информационная панель MaxPatrol VM отображает данные об активах и уязвимостях, обеспечивая специалистам полный контроль над ситуацией.

При оценке рисков MaxPatrol VM использует как стандартную систему CVSS, так и собственные алгоритмы, ориентируясь на угрозы, наиболее критичные для бизнеса.

- R-Vision VM от компании R-Vision.

Отличается гибкостью настроек сканирования, что позволяет адаптировать сервис под конкретные потребности организации. Платформа использует протоколы TCP/UDP для проверки доступности сервисов, что оптимизирует работу с крупными инфраструктурами.

Также, как и MaxPatrol VM, помимо CVSS имеет собственный контекстный анализ для оценки риска, учитывающий особенности активов.

Интеграция с SIEM и EDR системами, а также совместимость с системами управления конфигурациями, позволяет R-Vision VM создать комплексную систему защиты.

2. Сервисы управления уязвимостями.

Аутсорсинговые услуги от внешних провайдеров. Эти сервисы охватывают весь цикл управления уязвимостями: от обнаружения до устранения. Такой подход позволяет компаниям делегировать часть задач сторонним экспертам, обладающим необходимыми ресурсами.

Примеры Российских сервисов на рынке: Solar CPT и BI.ZONE.

- Solar CPT от компании ГК Солар.

Централизованный сервис, ориентированный на сети компаний и государственных организаций. Обеспечивает непрерывное тестирование на проникновение, поддерживает активное и пассивное сканирование. Работает с протоколами FTP и SMB. Использует многоуровневую систему оценки уязвимостей устройств и серверов, учитывающую критичность каждого актива для организации.

- BI.ZONE от компании CPT (Continuous Penetration Testing).

Поддерживает активное и пассивное сканирование, анализируя распространённые протоколы, такие как FTP и HTTPS.

Управление уязвимостями – это непрерывный процесс, требующий регулярного внимания и обновления знаний. В условиях цифровизации и глобализации важно не только осознавать риски, связанные с использованием данных, но и своевременно совершенствовать инструменты по их защите. Комплексный подход к информационной безопасности поможет организациям эффективно защищать свои данные и минимизировать потенциальные угрозы.

Список использованных источников:

1. Всё об управлении уязвимостями в 2025: Vulnerability Management. – URL: https://blog.infra-tech.ru/upravlenie-uyazvimostyami/ (дата обращения: 27.02.2025). – Текст: электронный.

2. What is Vulnerability Management and why is it important? – URL: https://www.threatlocker.com/blog/what-is-vulnerability-management (дата обращения: 27.02.2025). – Текст: электронный.

3. Системы управления уязвимостями: обзор технологии и российских продуктов. – URL: https://www.securitylab.ru/blog/personal/paragraph/354218.php (дата обращения: 27.02.2025). – Текст: электронный.