I. Введение

В документе "Health-ISAC: Risk-Based Approach to Vulnerability Prioritization", обсуждается важность определения приоритетов уязвимостей в управлении кибербезопасностью и подчёркивается необходимость совершенствования процессов управления уязвимостями и отказа от классических решений и систем. Вместо этого предлагается, чтобы организации внедряли решения, помогающие в расстановке приоритетов и управлении уязвимостями.

Этот документ подлежит тщательному анализу с уделением особого внимания многогранным аспектам управления уязвимостью в секторе здравоохранения. В ходе анализа будут рассмотрены стратегии и структуры, рекомендованные для эффективного определения приоритетов уязвимостей, задача, которая становится все более сложной.

Этот документ содержит практическое руководство по определению приоритетов уязвимостей. Хотя у него есть некоторые недостатки и ограничения, он может стать ценным ресурсом для организаций, стремящихся улучшить свои процессы.

A. Преимущества

- **Риск-ориентированный подход**: в документе подчёркивается риск-ориентированный подход к управлению уязвимостями, который может помочь организациям сосредоточиться на наиболее критичных из них, представляющих наибольшую угрозу
- **Полнота изложения**: документ включает различные методы, такие как базовая оценка CVSS, с упором на известные эксплуатируемые уязвимости, с учётом контекста устройства или размещения, стоимости активов, компенсирующих элементов управления и с использованием таких инструментов, как EPSS (система оценки прогнозирования эксплойтов) и SSVC (классификация уязвимостей для конкретных заинтересованных сторон)
- **Практическое руководство**: документ предлагает практическое руководство по внедрению этих методов и инструментов, облегчающее организациям внедрение этих практик

B. Недостатки

- **Ресурсоёмкость**: внедрение методов и инструментов, предложенных в документе, может быть ресурсоёмким, требующим значительного времени, усилий и опыта
- **Сложность**: подход документа сложен, и его внедрение может оказаться сложной задачей для небольших организаций или тех, у кого менее зрелые команды безопасности

C. Ограничения

- **Зависимость от точных данных**: эффективность методов и инструментов, предложенных в документе, зависит от доступности и точности данных. Например, для определения приоритета стоимости активов требуется точная и согласованная величина воздействия на бизнес для каждой компании
- **Динамический ландшафт угроз**: подход документа может не учитывать динамический характер ландшафта угроз. Постоянно появляются новые уязвимости и угрозы, которые могут потребовать внесения корректив в структуру расстановки приоритетов
- **Человеческий фактор**: хотя в документе предлагаются методы устранения человеческого фактора при определении приоритетов, человеческое суждение по-прежнему имеет решающее значение во многих аспектах управления уязвимостями, например, определение эффективности компенсирующих средств контроля или интерпретация результатов таких инструментов, как EPSS и SSVC
- **Зависимость от оценки CVSS**: в документе обсуждается использование Общей системы оценки уязвимостей (CVSS) в качестве основы. Хотя CVSS является широко признанным стандартом, его критиковали за то, что он неточно отражает реальный риск уязвимостей. Документ признает это и предлагает использовать дополнительные инструменты, такие как система оценки прогнозирования эксплойтов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC), но зависимость от CVSS все ещё можно рассматривать как ограничение
- **Отсутствие практических примеров**: хотя документ предоставляет всеобъемлющую теоретическую основу для определения приоритетов уязвимостей, ему могли бы помочь более практические примеры или тематические исследования, иллюстрирующие, как эти концепции могут применяться в реальных сценариях

II. Концепции документа

Основные идеи:

- **Использование базовой оценки CVSS**: общая система оценки уязвимостей (CVSS) — это стандарт, используемый для оценки критичности и возможности использования уязвимостей. Однако только 2–7% всех опубликованных уязвимостей когда-либо использовались в реальном времени, часто из-за отсутствия расстановки приоритетов
- **Сосредоточение внимания на известных эксплуатируемых уязвимостях**: предлагается более риск-ориентированный подход с упором на известные эксплуатируемые уязвимости. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) опубликовало список известных уязвимостей с использованием эксплойтов (KEV), чтобы помочь организациям расставить приоритеты в их усилиях по исправлению
- **Контекст или размещение устройства**: сетевое местоположение устройства является критическим фактором при определении приоритета уязвимости. Уязвимости и неправильные настройки, связанные с Интернетом, всегда должны быть приоритетом, в то время как внутренние активы должны подпадать под сроки исправления по внутреннему соглашению об уровне обслуживания (SLA)
- **Стоимость активов**: стоимость активов является ещё одним важным фактором при определении приоритетов уязвимости, о чём должны быть поставлены в известности аналитики
- **Компенсирующие средства контроля**: в большинстве организаций используются многоуровневые средства контроля безопасности или стратегии углублённой защиты для предотвращения атак. Эти средства контроля безопасности должны затруднить использование уязвимостей
- **EPSS – Система оценки прогнозирования эксплойтов**: EPSS – это модель машинного обучения, которая предсказывает вероятность того, что уязвимость будет использована в реальности. Это помогает более эффективно расставлять приоритеты в усилиях по устранению уязвимостей
- **SSVC – с конкретными заинтересованными сторонами уязвимости классификации**: SSVC фокусируется на ценностях, включая недостаток безопасности эксплуатации состояние, его влияние на безопасность, и распространённость продуктов. Это улучшает процессы управления уязвимостями и учитывает интересы различных заинтересованных сторон

III. Использование базовой оценки CVSS

Рассматривается использование Общей системы оценки уязвимостей (CVSS) в качестве основы, особенно для организаций с небольшими группами безопасности или тех, кто находится на ранних стадиях разработки программы управления уязвимостями

- **Базовая оценка CVSS в качестве отправной точки**: для организаций с ограниченными ресурсами или тех, кто только начинает свою программу управления уязвимостями, хорошей отправной точкой может стать использование базовой оценки CVSS для определения приоритетов и устранения всех критических уязвимостей высокой степени критичности. Такой подход устраняет необходимость в человеческом суждении при определении приоритетов уязвимостей, что может быть полезно для небольших команд или тех, у кого несколько обязанностей
- **Ограничения базовой оценки CVSS**: хотя использование базовой оценки CVSS может быть хорошей отправной точкой, у неё есть свои ограничения. Например, группы по устранению неполадок могут быть столкнуться с огромным количеством проблем, на которых их просят сосредоточиться. Кроме того, субъекты угроз не всегда могут использовать уязвимости наивысшей степени критичности и вместо этого объединяют в цепочку несколько эксплойтов менее критичных уязвимостей для получения доступа к системам
- **Необходимость более риск-ориентированного подхода**: учитывая ограничения, связанные с использованием только базового скоринга CVSS предлагается более риск-ориентированный подход, который фокусируется на известных эксплуатируемых уязвимостях. Это значительно сокращает количество проблем, требующих немедленного внимания, и позволяет специалистам-практикам сосредоточиться на уязвимостях, представляющих наибольшую угрозу для организаций

Общая система оценки уязвимостей CVSS — это платформа, используемая для оценки критичности уязвимостей в системе безопасности. Для расчёта баллов используются три группы показателей: базовые, временные и показатели окружения:

- **Базовые показатели (Base Metrics)**: дают оценку в диапазоне от 0 до 10, которая отражает неотъемлемые характеристики уязвимости, которые постоянны с течением времени и в разных пользовательских средах. Они разделены на две группы: показатели возможности использования (такие как вектор атаки, сложность атаки, требуемые привилегии и взаимодействие с пользователем) и показатели воздействия (которые измеряют влияние на конфиденциальность, целостность и доступность)
- **Временные показатели (Temporal Metrics)**: отражают характеристики уязвимости, которые могут меняться со временем, но вне зависимости от среды пользователя. Они включают зрелость кода эксплойта, уровень исправления и достоверность отчётов. Показатели являются необязательными и используются для получения временной оценки, которая является модификацией базовой оценки
- **Показатели окружения (Environmental Metrics)**: позволяют пользователю настраивать оценку CVSS в зависимости от важности затронутого программного обеспечения, оборудования или

данных в его среде. Они включают потенциальный сопутствующий ущерб, целевое распространение, Требования к конфиденциальности, целостности и доступности. Показатели являются необязательными и используются для получения оценки, которая является дальнейшей модификацией временной оценки

Базовая оценка CVSS отличается от других оценок тем, что она учитывает только неотъемлемые, неизменные характеристики уязвимости. Напротив, временная оценка учитывает факторы, которые меняются с течением времени, например, был ли разработан эксплойт или доступен патч. Оценка окружения позволяет настраивать её в зависимости от важности затронутых активов в среде конкретного пользователя. Следовательно, хотя базовая оценка одинакова для всех, а другие оценки могут варьироваться в зависимости от времени и конкретной среды пользователя.

Все три показателя показатели влияют друг на друга в том смысле, что каждая следующая является модификацией предыдущей: временная оценка является модификацией базовой оценки, а оценка окружения является модификацией временной оценки. Однако изменения в показателях окружения не влияют на другие оценки, поскольку это зависит от среды пользователя.

Базовая оценка общей системы оценки уязвимостей (CVSS) обычно не меняется с течением времени. Это статическая оценка, которая отражает критичность уязвимости на основе характеристик самой уязвимости, таких как её воздействие и возможность использования. Однако интерпретация и применение оценки CVSS может меняться с течением времени в зависимости от различных факторов.

Например, оценка CVSS может использоваться по-разному в контексте процесса управления уязвимостями организации. Организация может определять приоритетность уязвимостей не только на основе оценок уязвимостей CVSS, но и на основе таких факторов, как то, активно ли используется уязвимость, стоимость активов, которые могут быть затронуты, наличие компенсирующих элементов управления и контекст устройства.

Более того, в дополнение к оценке CVSS могут использоваться такие инструменты, как система оценки прогнозирования эксплойтов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC). EPSS использует модель машинного обучения для прогнозирования вероятности того, что уязвимость будет использована в реальности, обеспечивая динамический взгляд на риск, связанный с уязвимостью. SSVC, с другой стороны, фокусируется на ценностях, включая статус использования уязвимости, её влияние на безопасность и распространённость затронутых продуктов, что позволяет применять более индивидуальный подход к управлению.

IV. Сосредоточение внимания на известных эксплуатируемых уязвимостях

Подчёркивается важность определения приоритетности известных эксплуатируемых уязвимостей при управлении рисками кибербезопасности.

- **Известные эксплуатируемые уязвимости**: в отчёте предлагается подход, основанный на оценке рисков, который фокусируется на известных эксплуатируемых уязвимостях. Подчёркивается, что менее 4% всех известных уязвимостей использовались злоумышленниками, поэтому сосредоточение внимания на них может значительно сократить количество уязвимостей, требующих немедленного внимания
- **Определение приоритетов**: в отчёте предполагается, что известные эксплуатируемые уязвимости должны быть главным приоритетом для исправления. Такой подход гарантирует, что специалисты сосредоточат своё внимание на уязвимостях, которые представляют наибольшую угрозу. Процесс, обеспечивающий безопасность организации, будет включать в себя сосредоточение внимания на списке известных эксплуатируемых уязвимостей (KEV) CISA и поворот к устранению с критическими уровнями критичности
- **Уменьшение количества уязвимостей:** эта методология значительно сокращает количество уязвимостей, требующих немедленного внимания. По состоянию на 13 июля 2023 года в списке насчитывалось менее 1000 уязвимостей. Это также позволяет специалистам сосредоточиться на уязвимостях, представляющих наибольшую угрозу для организаций
- **Обязательства по соблюдению требований**: в отчёте также отмечается, что, хотя директива помогает агентствам расставлять приоритеты в своей работе по исправлению, она не освобождает их от каких-либо обязательств по соблюдению требований, включая устранение других уязвимостей
- **Оценка CVSS**: в отчёте признается, что оценка CVSS всё ещё может быть частью усилий организации по управлению уязвимостями, особенно при межмашинной коммуникации и крупномасштабной автоматизации

Сосредоточение внимания на известных эксплуатируемых уязвимостях является важнейшим аспектом. Это позволяет организациям эффективно распределять ресурсы, снижать риски, разрабатывать эффективные стратегии, соблюдать нормативные акты, определять приоритеты с учётом угроз и защищать ценные активы:

- **Эффективное распределение ресурсов**: ежегодно выявляются тысячи уязвимостей, и организациям часто бывает трудно управлять всеми и устранять их из-за ограниченности ресурсов. Сосредоточение внимания на известных эксплуатируемых

уязвимостях позволяет организациям уделять приоритетное внимание своим усилиям и ресурсам

- **Снижение риска**: известные эксплуатируемые уязвимости — это те, которые использовались злоумышленниками в реальности. Определяя приоритетность этих уязвимостей, организации могут значительно снизить свою подверженность риску.
- **Эффективные стратегии смягчения последствий и исправления ситуации**: определение приоритетности известных эксплуатируемых уязвимостей способствует разработке эффективных стратегий смягчения последствий и исправления ситуации. Это помогает командам безопасности эффективно взаимодействовать с заинтересованными сторонами, определять стоимость активов и разрабатывать политики исправления, способствующие непрерывности работы критически важных для бизнеса систем
- **Соответствие нормативным требованиям**: регулирующие органы, такие как Агентство по кибербезопасности и инфраструктурной безопасности (CISA), имеют директивы, направленные на снижение риска известных эксплуатируемых уязвимостей.
- **Определение приоритетов на основе угроз**: сосредоточение внимания на известных эксплуатируемых уязвимостях позволяет применять основанный на угрозах подход к управлению уязвимостями.
- **Защита активов**: определение приоритетности известных эксплуатируемых уязвимостей помогает защитить ценные активы. Если устройство, имеющее первостепенное значение для функционирования бизнеса или содержащее критически важную информацию, будет скомпрометировано, это может иметь катастрофические последствия для организации

V. Контекст, или размещение, устройства

- **Важность сетевого местоположения**: это знания имеют решающее значение для определения приоритетности уязвимостей, особенно когда речь идёт про уязвимости нулевого дня в отношении «активов», подключённых к Интернету
- **Определение приоритетности уязвимостей, связанных с Интернетом**: уязвимости и неправильные конфигурации на устройствах, подключённых к Интернету, должны быть приоритетными, поскольку они более доступны для субъектов угроз и могут служить лёгкой отправной точкой для атак. Эти уязвимости представляют собой более высокий риск компрометации и должны быть устранены незамедлительно
- **Сроки исправления внутреннего соглашения об уровне обслуживания**: для систем, которые недоступны из Интернета, таких как внутренние активы, рекомендуется, чтобы они подпадали под сроки исправления внутреннего соглашения об уровне обслуживания (SLA). Это означает, что в зависимости от сетевого расположения активов должны устанавливаться различные SLA, при этом активы, подключённые к Интернету, имеют более короткие SLA, чем внутренние
- **Использование рейтингов приоритета уязвимостей**: большинство инструментов управления уязвимостями сегодня включают дополнительные функции оценки, такие как система оценки прогнозирования эксплойтов (EPSS), для оказания помощи аналитикам в определении приоритетов уязвимостей. Эти инструменты предоставляют рейтинги приоритета уязвимости, которые помогают определить, какие недостатки безопасности следует устранить в первую очередь, исходя из вероятности использования в сети
- **Риск-ориентированный подход**: учитывая контекст определения местоположения устройства, организации могут действовать в соответствии с риск-ориентированным подходом к управлению уязвимостями. Такой подход гарантирует, что группы по исправлению ошибок сосредоточатся на устранении уязвимостей в зависимости от их вектора атаки, возможности использования и критичности

В контексте управления уязвимостями "контекст устройства или размещение" относится к сетевому местоположению и роли устройств, что является критическим фактором при определении приоритетов уязвимостей. Размещение устройства может существенно повлиять на уровень риска уязвимости и, следовательно, на расстановку приоритетов при усилиях по устранению неполадок.

A. Примеры размещения в системе управления уязвимостями

- **Реагирование на возникающие угрозы**: организациям необходимо быстро реагировать на возникающие угрозы или критические уязвимости на общедоступных устройствах. Например, если обнаруживается новая уязвимость, затрагивающая веб-серверы, эти серверы, подключённые к Интернету, будут иметь приоритет для исправления
- **Внутренние веб-приложения**: хотя это также важно, уязвимости, влияющие на внутренние веб-приложения, могут быть устранены позже уязвимостей на серверах, подключённых к Интернету
- **Рабочие станции или сервера**: локальная уязвимость с повышением привилегий может иметь приоритет на рабочих станциях над серверами, если рабочие станции с большей вероятностью станут мишенью для фишинговых писем, учитывая контекст использования устройств

VI. Ценность активов

Обсуждается важность понимания ценности актива в контексте определения приоритетов в отношении уязвимости.

- **Важность стоимости актива**: стоимость актива играет решающую роль в определении приоритетов уязвимости. Аналитикам необходимо понимать ценность актива в сочетании с его контекстом и размещением в сети. Это помогает определить приоритеты уязвимостей, связанных с критическими активами
- **Система ранжирования**: команды могут использовать систему ранжирования в своём репозитории приложений для определения критически важных ресурсов. Уязвимости, связанные с этими критически важными активами, должны быть приоритетными для устранения. Такой подход помогает аналитикам влиять на решения по устранению уязвимостей
- **Влияние на бизнес**: если устройство, имеющее решающее значение для функционирования бизнеса или содержащее критически важную информацию, будет скомпрометировано, это может иметь катастрофические последствия для организации. Поэтому рекомендуется уделять приоритетное внимание исправлению этих устройств по сравнению с другими. Учёт влияния на бизнес при оценке степени критичности обеспечивает более точное представление о риске для компании
- **База данных управления конфигурациями (CMDB)**: для эффективной реализации этой стратегии необходима точная и согласованная величина воздействия на бизнес для каждого актива компании. В идеале эта информация должна располагаться централизованно, например, в базе данных управления конфигурацией (CMDB). Хотя большинство отраслевых продуктов CMDB предоставляют решение для обнаружения активов, помогающее поддерживать точность инвентаризации, оно лишь частично избавляет от проблем

В управлении уязвимостями стоимость активов относится к важности конкретного актива (такого как устройство, система или данные) для операций организации или непрерывности бизнеса. Это важный фактор при определении приоритетов уязвимостей, помогающий командам безопасности решать, какие уязвимости следует устранить в первую очередь, исходя из потенциального воздействия на наиболее ценные активы организации.

Расчёт стоимости активов при управлении уязвимостями не является простым процессом и может варьироваться в зависимости от конкретного контекста и потребностей организации. Это часто включает оценку роли актива в организации, чувствительности хранящихся в нем данных, их важности для бизнес-операций и потенциального воздействия на организацию, если актив будет скомпрометирован.

На стоимость активов при управлении уязвимостями могут повлиять несколько факторов:

- **Роль актива**: функция актива в организации может в значительной степени влиять на его стоимость. Например, сервер, на котором размещены критически важные приложения или конфиденциальные данные, обычно имеет более высокую стоимость активов, чем периферийное устройство, не имеющее доступа к конфиденциальной информации
- **Конфиденциальность данных**: активы, которые хранят или обрабатывают конфиденциальные данные, такие как персональные данные информация (PII), финансовые данные или служебная деловая информация, обычно имеют более высокую ценность из-за потенциального воздействия утечки данных
- **Влияние на бизнес**: потенциальное воздействие на бизнес-операции в случае компрометации актива является важным фактором. Это может включать финансовые потери, сбои в работе, ущерб репутации или юридические и нормативные последствия
- **Размещение актива**: расположение актива в сети и подверженность потенциальным угрозам также могут влиять на его стоимость. Например, активы, которые являются общедоступными или расположены в демилитаризованной зоне (DMZ), могут считаться более ценными из-за повышенного риска стать мишенью для злоумышленников
- **Компенсирующие средства контроля**: наличие средств контроля безопасности, которые могли бы смягчить воздействие уязвимости, также может повлиять на предполагаемую стоимость актива. Например, актив с надёжными средствами контроля безопасности может считаться менее ценным с точки зрения управления уязвимостями, поскольку риск успешной эксплуатации снижается

Чтобы эффективно определять приоритеты уязвимостей на основе стоимости активов, организациям необходимо вести точную инвентаризацию и регулярно оценивать их стоимость в контексте деятельности организации и терпимости к рискам

VII. Компенсирующие элементы управления

Обсуждается роль многоуровневых средств контроля безопасности или стратегий углублённой защиты в смягчении последствий атак, выполняемых с помощью продвинутых угроз безопасности.

- **Компенсирующие элементы управления**: это меры безопасности, которые затрудняют использование уязвимостей. Они являются частью многоуровневой стратегии безопасности организации, также известной как стратегия углублённой защиты
- **Разногласия по поводу корректировки критичности**: практика корректировки критичности уязвимостей на основе компенсирующих средств управления является противоречивой. Некоторые заинтересованные стороны выступают за их снижение, исходя из предположения, что контроль эффективен. Однако изменение критичности уязвимости или рейтинга

риска без достаточных данных может привести к неправильному определению приоритетов и ослабить систему обеспечения безопасности организации.

- **Тестирование компенсирующих элементов управления**: в отчёте рекомендуется протестировать использование уязвимостей в стеке безопасности компании в изолированной среде. Это может быть сделано персоналом, имеющим опыт работы в redteam, или с помощью инструмента моделирования взломов и атак, имитирующего TTP, наблюдаемые при вредоносных операциях. Эти данные могут помочь определить, можно ли увеличить критичность или рейтинг риска определённых уязвимостей

Компенсирующие средства контроля при управлении уязвимостями — это дополнительные меры безопасности, применяемые для снижения риска, связанного с выявленными уязвимостями. Они используются, когда уязвимости не могут быть немедленно устранены из-за технических ограничений, бизнес-требований или других факторов. Компенсирующие средства контроля могут помочь определить приоритеты уязвимостей за счёт снижения риска, позволяя организациям в первую очередь сосредоточиться на устранении уязвимостей с более высоким уровнем риска.

Компенсирующие элементы управления могут принимать различные формы, включая:

- **Сегментация сети**: это включает разделение сети на несколько сегментов, чтобы ограничить способность злоумышленника перемещаться в поперечном направлении внутри сети. Если уязвимость существует в одном сегменте сети, сегментация сети может помешать злоумышленнику использовать эту уязвимость
- **Брандмауэры и системы предотвращения вторжений (IPS)**: эти инструменты могут обнаруживать и блокировать вредоносный трафик, потенциально предотвращая использование определённых уязвимостей
- **Многофакторная аутентификация (MFA)**: MFA может помешать злоумышленнику получить доступ к системе, даже если он получил действительные учётные данные, тем самым снижая риск, связанный с уязвимостями, которые могут привести к краже учётных данных
- **Шифрование**: шифрование хранимых и передаваемых данных может снизить воздействие уязвимостей, которые могут привести к раскрытию данных
- **Регулярное исправление и обновления систем:** регулярное обновление и исправление систем может помочь снизить риск, связанный с известными уязвимостями
- **Обучение по повышению осведомлённости о безопасности**: обучение пользователей с целью распознавать потенциальные угрозы безопасности и избегать их может снизить риск использования уязвимостей с помощью атак социальной инженерии

Что касается определения приоритетов уязвимостей, компенсирующие средства контроля могут использоваться для снижения рейтинга риска определённых уязвимостей, позволяя организациям в первую очередь сосредоточиться на устранении других уязвимостей. Однако важно отметить, что эффективность компенсирующих средств контроля должна регулярно проверяться, чтобы убедиться, что они функционируют должным образом, например redteam.

Помимо компенсирующих средств контроля, другие факторы, которые можно использовать для определения приоритетности уязвимостей, включают критичность уязвимости, возможность использования уязвимости, стоимость актива, на который влияет уязвимость, и известно ли, что уязвимость используется в реальности. Такие инструменты, как система оценки прогнозирования эксплойтов (EPSS) и классификация уязвимостей для конкретных заинтересованных сторон (SSVC), также могут быть использованы для определения приоритетности уязвимостей

Разница между компенсирующими элементами управления и исправлениями в управлении уязвимостями.

В контексте управления уязвимостями компенсирующий контроль и исправление — это две разные стратегии, используемые для снижения риска, связанного с выявленными уязвимостями.

Исправление относится к процессу применения обновлений к программному обеспечению или системам для устранения известных уязвимостей. Это прямой метод устранения, поскольку он включает в себя модификацию системы или программного обеспечения. Исправление часто является наиболее эффективным способом предотвращения использования уязвимости, но оно также может быть ресурсоёмким и разрушительным, поскольку может потребовать перевода систем в автономный режим или перезапуска. Также важно отметить, что не для всех уязвимостей доступны исправления, и даже если они есть, их применение может быть отложено из-за требований к тестированию или операционных ограничений.

С другой стороны, компенсирующие средства контроля — это альтернативные меры, применяемые для снижения риска, связанного с уязвимостью, когда применение исправления невозможно или желательно. Эти средства контроля не устраняют саму уязвимость, но снижают риск использования. Примеры компенсирующих средств контроля включают сегментацию сети, правила брандмауэра, системы обнаружения вторжений и дополнительный мониторинг. Использование компенсирующих средств контроля может быть спорным, поскольку они не устраняют уязвимость и их эффективность может быть трудно измерить. Однако они могут быть ценным инструментом управления рисками, особенно в случаях, когда немедленное исправление невозможно.

В то время как исправление непосредственно направлено на устранение уязвимостей, компенсирующие

элементы управления предоставляют альтернативные способы снижения риска, связанного с уязвимостями, когда исправление неосуществимо или желательно. Обе стратегии являются важными компонентами комплексной программы управления уязвимостями.

VIII. EPSS

EPSS — это инструмент, который помогает определять приоритеты уязвимостей в сфере кибербезопасности, представляющий оценку вероятности использования на основе данных, которая может дополнять традиционные рейтинги критичности и другие стратегии управления уязвимостями.

- **Проблемы с традиционной системой оценки**: традиционные системы оценки уязвимостей, такие как CVSS, подвергались критике за недостаточность для оценки рисков, связанных с уязвимостями, и определения их приоритетности с учётом фактора, что не все опубликованные эксплоиты находили подтверждение эксплуатации или были пригодны
- **Внедрение EPSS**: EPSS — это решение на основе данных и модели машинного обучения для прогнозирования вероятности того, что уязвимость будет использована в реальности. Это помогает более эффективно расставлять приоритеты в усилиях по устранению уязвимости. EPSS использует различные данные, например список CVE MITRE, данные о CVE, такие как количество дней с момента публикации, и наблюдения за эксплуатацией в реальных условиях
- **Оценка EPSS**: модель EPSS выдаёт оценку вероятности от нуля до единицы (от 0 до 100%). Чем выше оценка, тем больше вероятность того, что уязвимость будет использована
- **Сравнение с CVSS**: EPSS предназначен не для замены CVSS, а для дополнения его. В то время как CVSS предоставляет оценку критичности уязвимостей, EPSS обеспечивает прогнозирование вероятности использования. Эта дополнительная информация может помочь организациям более эффективно расставить приоритеты в своих усилиях по исправлению положения
- **Использование EPSS в управлении уязвимостями**: EPSS можно использовать в сочетании с другими инструментами и стратегиями управления уязвимостями, такими как поиск известных эксплуатируемых уязвимостей, учёт размещения устройств, оценка стоимости активов и применение компенсационных средств контроля
- **Категоризация уязвимостей для конкретных заинтересованных сторон (SSVC)**: SSVC — это ещё один инструмент, который можно использовать совместно с EPSS. SSVC фокусируется на таких аспектах, включая статус использования уязвимости в системе безопасности, её влияние на безопасность и распространённость затронутых продуктов. SSVC улучшает процессы управления уязвимостями и учитывает интересы различных заинтересованных сторон

A. Разница в EPSS с другими инструментами

EPSS предлагает более тонкий подход к управлению уязвимостями, прогнозируя вероятность использования, что дополняет оценку критичности, предоставляемую традиционными системами оценки, такими как CVSS. Эта возможность прогнозирования может принести значительную пользу организациям при определении приоритетности их усилий по устранению уязвимостей.

EPSS отличается от традиционных оценок критичности по ряду признаков:

- **Прогностический характер:** EPSS является прогностическим, предоставляя оценку вероятности, основанную на вероятности использования, в то время как CVSS предоставляет оценку критичности, связанную с внутренними характеристиками уязвимости
- **Подход, основанный на данных:** EPSS использует технологию, которая включает текущую информацию об угрозах из CVE и данные о реальных эксплойтах, чего нельзя сказать о рейтингах критичности CVSS
- **Модель машинного обучения:** EPSS использует модель машинного обучения для прогнозирования вероятности использования, используя данные из таких источников, как список MITRE CVE, и наблюдения за эксплуатацией в реальном времени от поставщиков безопасности

Преимущества использования EPSS для управления уязвимостями включают:

- **Эффективная расстановка приоритетов**: EPSS помогает организациям определять приоритеты уязвимостей, которые представляют наибольший риск и с наибольшей вероятностью будут использованы, позволяя им более эффективно распределять ресурсы
- **Дополнение к CVSS**: EPSS можно использовать наряду с CVSS для получения более полного представления об уязвимостях с учётом как критичности, так и вероятности эксплуатации
- **Сокращение усилий по устранению неполадок**: сосредоточив внимание на уязвимостях с более высокой вероятностью использования, организации могут сократить количество уязвимостей, которые им необходимо устранить, экономя время и усилия.

IX. SSVC

SSVC — это гибкий, настраиваемый и основанный на фактических данных подход к определению приоритетов уязвимостей. Это помогает организациям принимать обоснованные решения о том, какие уязвимости следует устранить в первую очередь, исходя из их конкретного контекста и толерантности к риску.

- **Обзор SSVC**: SSVC — это методология анализа уязвимостей, разработанная Институтом программной инженерии Университета Карнеги-Меллон в координации с Агентством США по кибербезопасности и инфраструктурной безопасности (CISA). Он работает как дерево решений, что обеспечивает гибкость в его

применении и учитывает интересы различных сторон.

- **Точки принятия решений SSVC**: SSVC использует дерево решений для определения реакции на уязвимость. Возможными результатами являются Track, Track*, Attend, и Act. У каждого результата есть рекомендуемый график исправления, начиная от стандартных сроков обновления (Track, Track*) и заканчивая немедленными действиями (Act).
- **Настраиваемость**: SSVC настраивается, помогая аналитикам принимать решения о действиях по устранению уязвимостей в соответствии с сохранением конфиденциальности, целостности и доступности корпоративных систем по согласованию с руководством.
- **Решения, основанные на фактических данных**: Решения SSVC основаны на логической комбинации триггеров, установленных руководством в ответ на такие факторы, как степень использования уязвимости, уровень сложности её использования противником и её влияние на общественную безопасность. Аналитики собирают данные о соответствующих триггерах и используют логику дерева решений для определения приоритетных решений по сортировке.
- **Расширение базовых оценок**: SSVC выходит за рамки просто базовых оценок как отдельный метод расстановки приоритетов. Это помогает организациям эффективно определять приоритеты и сортировать уязвимости, ориентируясь при этом в условиях неопределённости относительно того, какие проблемы следует решать в первую очередь.

A. Ключевые компоненты методологии SSVC

Ключевые компоненты методологии SSVC включают:

- **Точки принятия решения**: SSVC использует дерево решений с точками принятия решений, которые приводят к различным результатам на основе анализа уязвимости. Эти точки принятия решений включают состояние эксплуатации, техническое воздействие, автоматизируемость, распространённость миссии и влияние на общественное благосостояние.
- **Возможные результаты**: Дерево решений приводит к одному из четырёх возможных результатов: Track, Track*, Attend, и Act. Для каждого результата указаны рекомендуемые сроки исправления, при этом "Act" требует немедленных действий.
- **Настраиваемость**: SSVC разработан таким образом, чтобы его можно было настраивать, позволяя организациям адаптировать процесс принятия решений к их конкретным потребностям.
- **Решения, основанные на фактических данных**: Решения в рамках SSVC принимаются на основе доказательств, касающихся статуса эксплуатации уязвимости, сложности и воздействия на общественную безопасность.
- **Динамическое приложение**: SSVC задуман как концепция динамического применения, при этом выпускаются новые версии, включающие улучшения и отзывы.

B. Использование SSVC для определения приоритетов уязвимостей

SSVC может быть использован для эффективной расстановки приоритетов уязвимостей с помощью

- **Оценка воздействия**: анализ влияния уязвимости на деятельность организации и общественное благосостояние для определения срочности устранения.
- **Оценка состояния эксплуатации**: рассмотрение вопроса о том, имеется ли активная эксплуатация или подтверждение концепции уязвимости.
- **Определение автоматизируемости**: оценка того, является ли уязвимость самораспространяющейся или требует дополнительных действий для использования злоумышленником.
- **Принятие обоснованных решений**: использование дерева решений для принятия обоснованных решений о том, какие уязвимости следует устранить в первую очередь, на основе конкретного уровня уязвимости организации и рекомендуемых действий.

C. Разница между SSVC и традиционными оценками критичности в управлении уязвимостями

Традиционные системы оценки в управлении уязвимостями, такие как CVSS, предоставляют числовую оценку для обозначения критичности уязвимости. Эти оценки основаны на наборе показателей, которые, среди прочего, включают вектор атаки, сложность атаки, требуемые привилегии и взаимодействие с пользователем. Однако эти традиционные решения подвергаются критике за то, что их недостаточно для оценки рисков, связанных с уязвимостями, и определения их приоритетности, поскольку в них не учитывается, использовалась ли уязвимость в реальности.

С другой стороны, классификация уязвимостей для конкретных заинтересованных сторон (SSVC) представляет собой более динамичный и гибкий подход к управлению уязвимостями. SSVC фокусируется на ценностях, включая статус использования уязвимости в системе безопасности, её влияние на безопасность и распространённость затронутых продуктов. SSVC даёт более полное представление о риске, связанном с уязвимостью, принимая во внимание такие факторы, как состояние эксплуатации, техническое воздействие, распространённость миссии и общественное благосостояние.

Хотя традиционные рейтинги обеспечивают стандартизированную оценку уязвимости, они не учитывают, её влияние на организацию. SSVC, с другой стороны, обеспечивает более комплексный и настраиваемый подход к управлению уязвимостями за счёт учёта более широкого спектра факторов.

D. Скоринг в методологии SSVC

Методология категоризации уязвимостей для конкретных заинтересованных сторон (SSVC) представляет собой процесс принятия решений о действиях по устранению уязвимостей. Методология

SSVC предусматривает четыре оценочных решения, которые являются:

- **Track**: уязвимость в настоящее время не требует принятия мер, но организация должна продолжать отслеживать её и повторно оценивать, если станет доступна новая информация. CISA рекомендует устранять уязвимости отслеживания в стандартные сроки обновления.
- **Track***: уязвимость имеет специфические характеристики, которые могут потребовать более тщательного мониторинга изменений. CISA рекомендует устранять уязвимости отслеживания * в стандартные сроки обновления.
- **Attend**: уязвимость требует внимания со стороны внутренних сотрудников организации на уровне надзора. Необходимые действия включают запрос помощи или информации об уязвимости и могут включать публикацию уведомления внутри компании и / или извне. CISA рекомендует устранять уязвимости Attend раньше стандартных сроков обновления.
- **Act**: уязвимость требует внимания со стороны внутренних сотрудников организации, на уровне надзора и руководства. Необходимые действия включают запрос помощи или информации об уязвимости, а также публикацию уведомления внутри компании и / или извне. Как правило, внутренние группы собираются для определения общего ответа, а затем выполняют согласованные действия. CISA рекомендует устранить уязвимости Act как можно скорее.

E. Примеры SSVC

Примеры применения SSVC:

- **Индивидуальное дерево решений**: настройка дерева решений, чтобы сосредоточиться на факторах состояния эксплуатации уязвимости, её влияние на безопасность и распространённости затронутых продуктов
- **Возможные результаты**: дерево решений SSVC приводит к одному из четырёх возможных результатов: Track, Track*, Attend, и Act. Для каждого результата указаны рекомендуемые сроки устранения, при этом "Act" требует немедленных действий. Это помогает организациям определять приоритеты уязвимостей в зависимости от уровня внимания, которого они требуют
- **Решения, основанные на фактических данных**: решения в рамках SSVC принимаются на основе доказательств, касающихся статуса эксплуатации уязвимости, сложности эксплуатации и воздействия на общественную безопасность. Например, если уязвимость активно используется с высоким техническим воздействием необходимо немедленное решение проблемы (Act)
- **Пример практического использования**: практический пример представляет собой ответ с определением приоритетов на уязвимость Citrix ShareFile, идентифицированную как CVE-2023-24489. Используя SSVC, организация, скорее всего, выбрала бы значение "Act" после сопоставления информации, собранной аналитиками, с точками принятия решений и связанными с ними значениями. На это решение влияет наличие кода, подтверждающего правильность концепции, свидетельства целенаправленных атак и использования в реальных условиях

X. Показатели

Обсуждается роль показателей в оценке и совершенствовании программы управления уязвимостями. Подчёркивается важность использования подробных и информативных показателей для оценки эффективности программы управления уязвимостями. Сосредоточившись на ключевых показателях риска и разделив показатели на отдельные группы, организации могут получить полезную информацию и более эффективно расставить приоритеты в усилиях по устранению последствий.

- **Показатели как индикаторы**: показатели необходимы для определения эффективности программы управления уязвимостями и выявления областей, требующих улучшения. Они обеспечивают способ измерения эффективности программы и принятия стратегических решений
- **Детализация**: простого подсчёта количества критических, уязвимостей высокой, средней и низкой критичности недостаточно, чтобы определить, достигают ли усилия по устранению поставленных целей. Показатели должны быть более детализированными и информативными
- **Разделение показателей**: показатели должны быть разделены по технологиям, размещению в сети и Соглашению об уровне обслуживания (SLA), изложенному в политике компании.
- **Фокус на известных эксплуатируемых уязвимостях**: различие между известными эксплуатируемыми уязвимостями и теми, которые в настоящее время не эксплуатируются, помогает направить усилия команды точечно на решение проблемы
- **Ключевые показатели риска и показатели эффективности**: организациям следует сосредоточиться на ключевых показателях риска, а не только на ключевых показателях эффективности. Такой подход позволяет получить конкретную информацию, полученную на основе данных об уязвимостях, которая может быть более применимой
- **Пример показателей, основанных на оценке рисков**: сравнение сроков устранения уязвимостей на разных платформах, таких как Chrome и Edge. Это сравнение может выявить, какая платформа представляет более высокий уровень риска, исходя из времени, необходимого для устранения уязвимостей