Аннотация – в документе представлен анализ модели зрелости Essential Eight, разработанной Австралийским центром кибербезопасности для усиления безопасности в организациях. Анализ охватывает различные аспекты модели, включая её структуру, проблемы внедрения и преимущества достижения различных уровней зрелости.

Анализ предлагает ценную информацию о её применении и эффективности. Этот анализ полезен специалистам по безопасности, ИТ-менеджерам и лицам, принимающим решения в различных отраслях с целью эффективного способа защиты организации от угроз и усиления мер безопасности.

I. Введение

Модель зрелости Essential Eight (E8MM) предоставляет подробные рекомендации и информацию для предприятий и государственных структур по внедрению и оценке методов обеспечения кибербезопасности.

- **Цель и аудитория**: разработан для оказания помощи малому и среднему бизнесу, крупным организациям и государственным структурам в повышении их уровня кибербезопасности.
- **Обновления контента**: впервые опубликовано 16 июля 2021 года и регулярно обновляется, последнее обновление от 23 апреля 2024 года и информация остаётся актуальной и отражает новейшие методы обеспечения кибербезопасности и угрозы.
- **Доступность ресурсов**: доступен в виде загружаемого файла под названием "Модель зрелости PROTECT - Essential Eight", что делает его доступным для автономного использования и простого распространения в организациях.
- **Механизм обратной связи**: использование пользовательских отзывов указывает на постоянные усилия по улучшению ресурса на основе пользовательского вклада.
- **Дополнения**: страница cyber.gov.au также предлагает ссылки для сообщения об инцидентах кибербезопасности, особенно для критически важной инфраструктуры, и для подписки на оповещения о новых угрозах, подчёркивая упреждающий подход к кибербезопасности.

II. Специфика

Подчёркивается упреждающий, основанный на учёте рисков подход к безопасности, отражающий меняющийся характер угроз и важность поддержания сбалансированного и всеобъемлющего подхода к безопасности

A. Общие вопросы

- **Кибер-восьмёрка**: восемь стратегий смягчения последствий, рекомендуемых организациям для внедрения в качестве основы для защиты от кибер-угроз. Этими стратегиями являются управление приложениями, исправление приложений, настройка параметров макросов Microsoft Office, защита пользовательских приложений, ограничение прав администратора, обновление операционных систем, многофакторная аутентификация и регулярное резервное копирование.
- **Цель внедрения**: внедрение рассматривается как упреждающая мера, которая является более рентабельной с точки зрения времени, денег и усилий по сравнению с реагированием на крупномасштабный инцидент кибербезопасности.
- **Модель зрелости**: модель помогает организациям внедрять её поэтапно, исходя из различных уровней профессионализма и целевой направленности.

B. Обновления модели зрелости

- **Причина обновлений**: обновление модели происходит для поддержания актуальности и практичности и основаны на развитии технологий вредоносного ПО, разведданных о кибер-угрозах и отзывах участников мероприятий по оценке и повышению эффективности модели.
- **Последние обновления**: последние обновления включают рекомендации по использованию автоматизированного метода обнаружения активов не реже двух раз в неделю и обеспечению того, чтобы сканеры уязвимостей использовали актуальную базу данных уязвимостей.

C. Обновление и внедрение модели зрелости

- **Переопределение уровней зрелости**: Обновление от июля 2021 года переопределило количество уровней зрелости и перешло к более жёсткому подходу к реализации, основанному на учёте рисков. Повторно введён Нулевой уровень зрелости, чтобы обеспечить более широкий диапазон рейтингов уровня зрелости.
- **Риск-ориентированный подход**: В модели теперь делается упор на риск-ориентированный подход, при котором учитываются такие обстоятельства, как устаревшие системы и техническая задолженность. Отказ от реализации всех стратегий смягчения

последствий, где это технически возможно, обычно считается Нулевым уровнем зрелости.

- **Комплексное внедрение**: Организациям рекомендуется достичь согласованного уровня зрелости по всем восьми стратегиям смягчения последствий, прежде чем переходить к более высокому уровню зрелости. Этот подход направлен на обеспечение более надёжного базового уровня, чем достижение более высоких уровней зрелости в нескольких стратегиях в ущерб другим.

D. Обновления конкретной Стратегии

- **Изменения в управлении приложениями**: для всех уровней зрелости введены дополнительные типы исполняемого содержимого, а первый уровень зрелости был обновлён, чтобы сосредоточиться на использовании прав доступа к файловой системе для предотвращения выполнения вредоносного ПО

III. Подход к кибербезопасности

Стратегии разработаны, чтобы работать согласованно и обеспечивать надёжную защиту от различных угроз. Организациям рекомендуется внедрять их таким образом, чтобы они соответствовали их конкретным потребностям и рискам, потенциально используя другие меры безопасности

- **Контроль приложений**: Ограничение выполнения вредоносного и неавторизованного ПО.
- **Исправление приложения**: регулярное обновление приложений для устранения уязвимостей в системе безопасности.
- **Microsoft Office**: Ограничение использования макросов для предотвращения доставки вредоносных программ через документы Office.
- **Защита пользовательских приложений**: уменьшение поверхности атаки за счёт отключения часто используемых функций, таких как Java, Flash и веб-реклама.
- **Ограничение привилегий**: Ограничение административных прав для уменьшения вероятности неправильного использования и ограничения объёма ущерба от атаки.
- **Исправление операционных систем**: регулярное обновление операционных систем для устранения уязвимостей.
- **Многофакторная аутентификация (MFA)**: требуются дополнительные методы проверки для усиления контроля доступа.
- **Регулярное резервное копирование**: Обеспечение регулярного резервного копирования данных и проверки резервных копий на предмет возможности их восстановления.

IV. Уровни зрелости

Организациям рекомендуется достичь согласованного уровня зрелости по всем восьми стратегиям смягчения последствий, прежде чем рассматривать вопрос о переходе на более высокий уровень. Это обеспечивает сбалансированный подход к кибербезопасности, сводя к минимуму слабые места, которыми могут воспользоваться злоумышленники.

Выбор целевого уровня зрелости должен основываться на риск-ориентированном подходе, принимая во внимание конкретные обстоятельства организации и меняющийся характер кибер-угроз, что позволяет эффективно расставлять приоритеты по обеспечению безопасности.

- **Нулевой уровень зрелости**: указывает на существенные недостатки в системе кибербезопасности организации, облегчающие её использование злоумышленниками.
- **Первый уровень зрелости**: нацелен на элементарную кибер-гигиену для защиты от злоумышленников с использованием широкодоступных инструментов и техник. Этот уровень подходит для организаций, стремящихся защитить себя от общих, нецелевых кибер-угроз.
- **Второй уровень зрелости**: обеспечивает более совершенную защиту от противников, которые готовы вкладывать больше усилий и ресурсов, нацеливаясь на конкретную организацию. Этот уровень предполагает более жёсткий контроль и более быстрое реагирование.
- **Третий уровень зрелости**: представляет собой наивысший стандарт кибербезопасности в рамках модели, направленный на защиту от высокопрофессиональных противников, которые нацелены на конкретные организации с использованием передовых тактик.

V. Преимущества достижения целевого уровня

Достижение каждого целевого уровня зрелости в не только укрепляет защиту организации от кибер-угроз, но и повышает её операционную эффективность, соответствие требованиям и стратегическое позиционирование на рынке

A. Усиленная защита

- **Снижение уязвимости к атакам**: Придерживаясь стратегий на целевом уровне зрелости, организации могут значительно снизить уязвимость к широкому спектру кибератак, включая вредоносное ПО, программы-вымогатели и фишинг.
- **Предотвращение утечек данных**: Эффективное выполнение рекомендаций помогает предотвратить несанкционированный доступ к конфиденциальной информации, тем самым защищая от утечек данных, которые могут иметь серьёзные финансовые и репутационные последствия.

B. Улучшение комплаенса и управления рисками

- **Соблюдение стандартов**: для госучреждений Австралии модель является обязательной через достижение целевого уровня зрелости. Для других организаций это соответствует лучшим практикам и может соответствовать или превосходить отраслевые стандарты, которые со временем могут стать более регламентированными.
- **Усовершенствованное управление рисками**: Достижение целевого уровня зрелости позволяет

организациям более эффективно управлять рисками, согласовывая меры кибербезопасности со своей склонностью к риску и ландшафтом угроз.

C. Эксплуатационные преимущества

- **Эффективность**: Реализация стратегий обеспечивает хорошую отдачу от инвестиций за счёт снижения потенциальных потерь от кибер-инцидентов.
- **Оптимизированное управление ИТ**: Организации, достигшие целевого уровня зрелости, имеют чётко определённые процессы и системы управления кибербезопасностью, что может привести к повышению эффективности ИТ-операций и сокращению времени простоя.

D. Стратегические преимущества

- **Репутация и доверие**: Организации с высоким уровнем зрелости в области кибербезопасности, могут укрепить доверие клиентов, партнёров, через повышение репутации.
- **Конкурентное преимущество**: достигая и поддерживая высокий уровень зрелости, организации могут получить конкурентное преимущество, особенно если кибербезопасность является важнейшим аспектом их бизнеса.

E. Долгосрочная устойчивость

- **Ориентированность на будущее**: Модель зрелости разработана быть адаптивной к изменениям в ландшафте угроз, а достижение целевого уровня зрелости подготавливает организации к быстрой адаптации к новым угрозам и технологиям, обеспечивая долгосрочную устойчивость к кибербезопасности

VI. Последние изменения

Недавнее обновление модели зрелости привнесло несколько существенных изменений, направленных на усиление мер безопасности на различных уровнях зрелости.

A. Исправление приложения и операционные системы

- **Повышенный приоритет при исправлении**: Организациям теперь настоятельно рекомендуется исправлять критические уязвимости в течение 48 часов. Основное внимание также было уделено исправлению приложений, взаимодействующих с ненадёжным контентом, в течение двух недель.
- **Регулярное сканирование уязвимостей**: Частота сканирования систем на наличие критических уязвимостей увеличена как минимум с двух раз в неделю до как минимум еженедельной.

B. Многофакторная аутентификация (MFA)

- **Повышенные требования MFA**: Добавлены более строгие требования MFA начиная с первого уровня зрелости. MFA теперь обязателен для веб-порталов, хранящих конфиденциальные данные, и для входа сотрудников в бизнес-системы.
- **Защищённый от фишинга MFA**: для повышения безопасности особое внимание уделяется внедрению защищённого от фишинга MFA.

C. Ограничить права администратора

- **Управление привилегированным доступом**: Усовершенствованные процессы управления привилегированным доступом включают необходимость в защищённых рабочих станциях администратора и идентификации и омрачению учётных записях, получающих доступ к Интернету,

D. Управление приложениями

- **Ежегодные проверки и списки блокировок**: Организации обязаны проводить ежегодные проверки наборов правил контроля приложений и внедрять рекомендуемый Microsoft список блокировок приложений на втором уровне зрелости.

E. Повышение надежности пользовательских приложений

- **Прекращение использования Internet Explorer 11**: Организации должны отключить или удалить Internet Explorer 11 по окончанию его поддержки. Также уделяется особое внимание внедрению строгих рекомендаций по усилению защиты от поставщиков на более высоких уровнях зрелости.

F. Регулярные резервные копии

- **Учёт важности данных**: несмотря на отсутствие существенных изменений в требованиях к резервному копированию, рекомендуется учитывать важность данных для бизнеса при определении приоритетов резервного копирования.

G. Ведение журнала

- **Централизованный журнал**: Требование к централизованному ведению журнала перенесено с уровня зрелости 3 на уровень зрелости 2, что существенно увеличит размер журналов.

H. Новые приоритетные области

- **Управление облачными сервисами и управление инцидентами**: они были добавлены в качестве новых приоритетных областей в обновлении, отражающих необходимость более эффективного управления облачными сервисами и более надёжного реагирования на инциденты.

I. Общие усовершенствования

- **Соответствие Руководству по информационной безопасности (ISM)**: В обновлении применён ISM, чтобы обеспечить согласованность между двумя фреймворками и облегчить автоматическое использование основных восьми инструментов отслеживания и отчётности с помощью инструментов управления, соответствия требованиям и отчётности