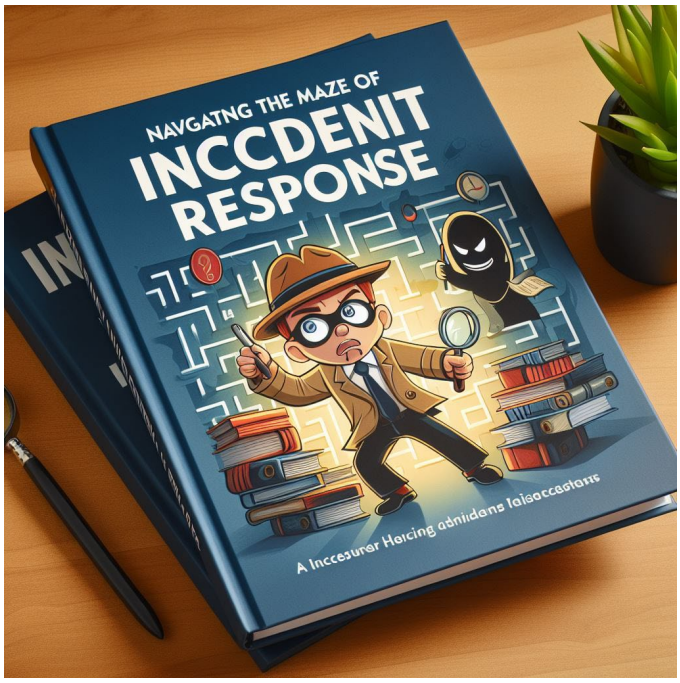

I. Введение

Документ Microsoft "Navigating Incident Response" представляет собой руководство, призванное помочь организациям разобраться в сложностях реагирования на инциденты (IR). В нем подчёркивается неизбежность инцидентов в области кибербезопасности и важность запуска IR с полным пониманием необходимых действий, сроков и вовлечённых сторон. В руководстве основное внимание уделяется людям и процессам, имеющим решающее значение для эффективного реагирования.

Углубляясь в анализ этого документа, ниже будет представлено качественное изложение его ключевых рекомендаций и стратегий, направленных на то, чтобы снабдить организации знаниями для быстрого сдерживания участников угроз и минимизации воздействия на бизнес, сохраняя при этом фактические данные и понимая соответствие требованиям и нормативные обязательства

II. Ключевые тезисы

A. *Ключевые моменты:*

- Инциденты кибербезопасности неизбежны, и наличие проработанного плана реагирования имеет решающее значение для быстрой локализации и восстановления
- Люди и процессы лежат в основе эффективного реагирования на инциденты с чёткими ролями, обязанностями и стратегиями управления
- Методологии реагирования на инциденты разработаны на базе и с использованием NIST
- Управление является ключевым, при этом такие роли, как руководитель управления, менеджер инцидентов и руководитель расследования, имеют решающее значение для структуры реагирования
- Коммуникация необходима, как внутренняя, так и внешняя, для управления сообщениями во время инцидента
- Сохранение и сбор доказательств являются приоритетными для проведения всестороннего расследования и составления полной картины инцидента
- Планирование смен и привлечение поставщиков важны для обеспечения поддержки в разных часовых поясах и со стороны сторонних ИТ-служб
- SITREP-отчёты обеспечивают активную коммуникацию с заинтересованными сторонами, поддерживая единый источник об инциденте
- Криминалистическое расследование должно быть скоординированным, с определением приоритетов задач на основе риска и включать упреждающий сетевой мониторинг
- Использование защищённых каналов взаимодействия для обеспечения конфиденциальности на период разрешения инцидентов
- При планировании восстановления следует учитывать долгосрочное восстановление и ужесточение службы на основе выявленных рисков и пробелов в безопасности
- Нормативные и юридические обязательства должны быть поняты и учтены на ранних стадиях процесса реагирования

B. *Основные выводы:*

- Только четверть организаций имеют постоянный план реагирования на инциденты
- Распространённые ошибки при реагировании на инциденты включают неэффективное устранение неполадок, непреднамеренное уничтожение доказательств, отсутствие документации и отказ от взаимодействия с поставщиками и юрисконсультом на раннем этапе
- Привлечение поставщика имеет решающее значение для сбора доказательств и поддержки во время инцидента, а упреждающее участие обеспечивает приоритизацию запросов
- Подходы к противодействию должны быть адаптированы к типу инцидента с учётом воздействия на бизнес и потенциального оповещения субъекта угрозы
- Активные коммуникации играют важную роль в контроле обмена данными и реагировании на запросы о предоставлении информации, обеспечивая последовательность и согласованность с расследованием
- Правовые и нормативные соображения сложны и варьируются в зависимости от юрисдикции, что требует заблаговременного привлечения юрисконсульта для представления обязательной отчётности и соблюдения требований

C. *Ключевые действия и точки приложения*

- **Создание структуры управления инцидентами**: в начале инцидента важно разработать модель реагирования для управления инцидентом. Это включает в себя определение ключевых заинтересованных сторон, которые могут помочь сформировать структуру реагирования
- **Определение потенциальных клиентов**: в руководстве предлагается определять потенциальных клиентов в различных рабочих потоках, таких как управление, контроль инцидентов, расследования, инфраструктура, коммуникация и соответствие нормативным требованиям
- **Вовлечение заинтересованных сторон**: руководящему составу следует заблаговременно уведомлять заинтересованные стороны и членов команды исполнительного руководства о реагировании на инциденты
- **Выделение ресурсов**: по возможности следует выделять ресурсы для реагирования или, как минимум, направлять на приоритизацию действий по реагированию по сравнению с другими задачами

D. *Лучшие практики*

- **Сохранение доказательств:** помимо понимания масштабов компромисса и способов восстановления контроля, важно сохранить доказательства и понимать обязательства по соблюдению нормативных требований.
- **Поддерживание прозрачности и понимания риска**: руководству следует осуществлять надзор за реагированием, чтобы иметь предметное представление о риске, связанном с инцидентом. Это должно поддерживаться на протяжении всего процесса реагирования с помощью отчётов о ситуации, подготовленных менеджером инцидентов
- **Взаимодействие с главными владельцами (ресурсов)**: руководитель управления должен оказывать поддержку, если группа реагирования сталкивается с проблемой, которая не может быть решена на оперативном уровне. Типичные проблемы могут включать запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также решения, которые имеют широкомасштабное влияние на бизнес
- **Управление рабочим потоком и распределение задач**: с какого-то момента документирование действий и задач часто утрачивает приоритетность в пользу быстрого реагирования. Но в дальнейшем это может создавать проблемы. Поэтому важно документировать действия и задачи с начала

III. План реагирования на инциденты

План реагирования на инциденты (IRP) – это структурированный подход к обработке инцидентов безопасности, брешей и киберугроз. Чётко определённый IRP может помочь организациям свести к минимуму потерю и кражу данных, смягчить последствия кибератак и сократить время восстановления и затраты. К ключевым компонентам IRP относятся:

- **Подготовка**: включает в себя создание группы реагирования на инциденты, определение их ролей и обязанностей, а также проведение необходимого обучения, подготовку необходимых инструментов и ресурсов для обнаружения инцидентов и реагирования на них.
- **Обнаружение**: этап включает выявление потенциальных инцидентов безопасности, обычно с помощью систем обнаружения вторжений, брандмауэров или систем предотвращения потери данных (DLP).
- **Локализация**: после обнаружения инцидента необходимо предпринять шаги для предотвращения дальнейшего ущерба. Это может включать изоляцию затронутых систем или сетей, чтобы предотвратить распространение инцидента.
- **Устранение**: включает в себя поиск основной причины инцидента и удаление затронутых систем из сети для проведения криминалистического анализа.
- **Восстановление**: восстановление и возвращение системы к нормальной работе возможно в отсутствии следов инцидента. Это может включать исправление программного обеспечения, очистку систем или даже переустановку целых систем.
- **Действия после инцидента**: после рассмотрения инцидента следует провести анализ для повышения эффективности реагирования в будущем. Это может включать обновление IRP, внедрение новых мер безопасности или проведение дополнительного обучения для персонала

При рассмотрении инструментов реагирования на инциденты организации должны учитывать несколько ключевых соображений для обеспечения эффективного реагирования на инциденты кибербезопасности:

A. *Интеграция с существующими системами*

Инструменты реагирования на инциденты должны быть способны легко интегрироваться с существующей инфраструктурой безопасности организации, такой как брандмауэры, системы обнаружения вторжений и решения SIEM. Такая интеграция позволяет осуществлять автоматический сбор и корреляцию данных, что может ускорить обнаружение и анализ инцидентов безопасности.

B. *Масштабируемость*

Инструменты должны быть масштабируемыми для обработки объёма данных и количества конечных точек внутри организации. По мере роста организации

инструменты должны быть способны обрабатывать все больший объем данных и расширять сеть без снижения производительности.

C. Сохранение доказательств

Во время инцидента сохранение улик имеет решающее значение для тщательного расследования и возможного криминалистического разбирательства. Инструменты реагирования на инциденты должны способствовать сбору и сохранению цифровых доказательств с точки зрения криминалистической экспертизы, гарантируя, что они остаются приемлемыми в суде, если это необходимо.

D. Мониторинг и оповещение в режиме реального времени

Возможность отслеживать сеть в режиме реального времени и формировать оповещения о подозрительных действиях имеет важное значение. Это позволяет быстро выявлять потенциальные угрозы и реагировать на них до того, как они смогут нанести значительный ущерб.

E. Автоматизация и управление

Автоматизация повторяющихся задач и координация ответных действий могут значительно повысить эффективность процесса реагирования на инциденты. Инструменты, обеспечивающие автоматизированные рабочие процессы, могут помочь сократить время на реагирование и смягчение последствий угроз, а также свести к минимуму вероятность человеческой ошибки.

F. Удобный интерфейс

Инструменты должны иметь интуитивно понятный и удобный интерфейс, позволяющий специалистам быстро ориентироваться и эффективно использовать функции, особенно в условиях активного инцидента.

G. Подробная отчетность

Инструменты должны обеспечивать комплексные возможности отчётности, позволяющие проводить подробный анализ и документировать инциденты. Это важно для анализа последствий, соблюдения нормативных требований и улучшения системы безопасности организации.

H. Индивидуальность и гибкость

У каждой организации свои уникальные потребности. Инструменты реагирования на инциденты должны настраиваться в соответствии с конкретными процессами организации. Они также должны быть достаточно гибкими, чтобы адаптироваться к меняющемуся ландшафту угроз и организационным изменениям.

I. Поддержка поставщиков и сообщества

Надёжная поддержка поставщиков и активное сообщество пользователей могут стать бесценными ресурсами для устранения неполадок, обмена передовым опытом и получения информации о последних угрозах и стратегиях реагирования.

J. Соблюдение требований законодательства и нормативов

Инструменты должны помочь организациям соблюдать правовые и нормативные требования, связанные с реагированием на инциденты, такие как обязательная отчётность и правила конфиденциальности. Это включает в себя функции, которые поддерживают управление нормативными / правовыми требованиями и облегчают взаимодействие с юрисконсультом, когда это необходимо.

IV. Роли и обязанности

Модифицированная версия модели жизненного цикла реагирования на инциденты, задокументированной Национальным институтом стандартов и технологий (NIST) обычно включает подготовку, обнаружение, локализацию, ликвидацию, восстановление и действия после инцидента или извлечённые уроки. В связи с этим предлагается модель реагирования для управления инцидентом, которая включает следующие роли:

- **Руководитель управления**: эту роль обычно выполняет CISO или CIO. Они поддерживают прозрачность рисков и влияние на бизнес в целом, а также общаются с высокопоставленными заинтересованными сторонами
- **Менеджер инцидентов**: эту роль обычно выполняет руководитель ITSM / операций по обеспечению безопасности. Он координирует все оперативные рабочие процессы для понимания и сдерживания угрозы, а также доводит информацию о риске до руководства
- **Руководитель расследования**: эту роль обычно выполняет старший специалист по информационным технологиям / старший представитель по ИТ-операциям. Он отвечает за понимание общего компромисса и информирование о связанных с ним рисках
- **Руководитель инфраструктуры**: эту роль обычно выполняет старший представитель по ИТ-операциям. Он несёт ответственность за сдерживание угрозы путём снижения риска, связанного с компромиссом
- **Менеджер по коммуникациям**: эту роль обычно выполняет специалист по коммуникациям. Он контролирует обмен данными как внешне, так и внутренне
- **Руководитель отдела регулирования**: эту роль обычно выполняет внутренний юрисконсульт / представитель GRC. Он отвечает за оценку рисков / воздействия и управление нормативными / правовыми требованиями для поддержания соответствия

Рекомендуемые наборы навыков для работы:

- **Руководитель управления**: оперативный надзор, поддержание прозрачности, понимание рисков и последствий, а также общение с

высокопоставленными заинтересованными сторонами

- **Менеджер инцидентов**: оперативное управление и постановка задач, координация всех операционных рабочих потоков и информирование руководства о рисках
- **Руководитель расследования**: криминалистическое расследование для понимания общего компромисса и информирования о связанных с ним рисках
- **Руководитель инфраструктуры**: сдерживание угроз за счёт снижения риска, связанного с компромиссом
- **Менеджер по коммуникациям:** вовлечение заинтересованных сторон и контроль обмена сообщениями как внешними, так и внутренними
- **Руководитель отдела регулирования**: Оценка рисков / последствий и управление нормативными / правовыми требованиями для поддержания соответствия

Обеспечение эффективного плана реагирования на инциденты:

- **Регулярное обновление плана**: обновление плана реагирования на инциденты с учётом меняющегося ландшафта угроз и организационных изменений
- **Тренинги**: проведение регулярных тренингов симуляций для проверки плана и определения областей для улучшения
- **Коммуникация**: установление и поддерживание чётких каналов коммуникации для всех заинтересованных сторон, участвующих в реагировании на инцидент
- **Документирование**: все действия и решения должны быть задокументированы, чтобы избежать путаницы и неэффективности
- **Взаимодействие с поставщиками**: активное взаимодействие с поставщиками для поддержки сбора доказательств и других мероприятий по реагированию
- **Планирование смен**: внедрение планирования смен, чтобы предотвратить выгорание и поддерживать непрерывное реагирование в различных временных зонах

A. Руководитель управления

Руководитель управления, которым может быть CISO или CIO, отвечает за оперативный надзор. Его роль заключается в поддержании прозрачности и понимании рисков и их влияния на бизнес в целом, а также в общении с высокопоставленными заинтересованными сторонами. Представитель этой роли должен заблаговременно уведомить заинтересованные стороны и членов команды исполнительного руководства о том, что принимаются серьёзные ответные меры. Это гарантирует, что другие подразделения бизнеса будут осведомлены о потенциальном риске и о том, что во время управления инцидентом могут произойти сбои в обслуживании.

Представитель роли также должен обеспечить выделение специальных ресурсов для принятия ответных мер. Организации, не имеющие выделенных групп безопасности, часто привлекают ресурсы из других подразделений бизнеса для оказания помощи в реагировании. Затем этим сотрудникам необходимо сбалансировать свою существующую рабочую нагрузку с мероприятиями по реагированию. По возможности, для реагирования следует выделять специальные ресурсы или, как минимум, направлять их на приоритизацию мероприятий по реагированию по сравнению с другой работой

Руководитель управления также является связующим звеном группы реагирования как с внутренними, так и с внешними высокопоставленными заинтересованными сторонами. Если группа реагирования сталкивается с проблемой, которая не может быть решена на оперативном уровне, представитель роли должен оказать поддержку. Типичные проблемы включают запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также утверждение решений, которые имеют широкомасштабные последствия для бизнеса, такие как массовый сброс паролей или отключение подключения к Интернету, и т.д.

B. Менеджер инцидентов

Менеджер инцидентов обычно является руководителем ITSM / операций по обеспечению безопасности, основными обязанностями которого являются оперативное управление и постановка задач. Эта роль включает в себя координацию всех операционных потоков работы для понимания, сдерживания и информирования Руководства об угрозе.

Менеджер инцидентов отвечает за управление и отслеживание задач для всех операционных рабочих потоков, чтобы обеспечить приоритетность и документирование действий.

Менеджер инцидентов также играет ключевую роль в поддержании прозрачности и понимания риска. Он готовит отчёты о ситуации для руководителя управления, чтобы иметь предметное представление о риске, связанном с инцидентом

В случае возникновения проблем, которые не могут быть решены на оперативном уровне, менеджер инцидентов инициирует запросы к руководству. Типичные проблемы, которые могут потребовать такого увеличения, включают запросы ресурсов от других подразделений бизнеса, увеличение количества запросов к поставщикам и другим третьим сторонам, а также решения, которые оказывают широкомасштабное влияние на бизнес, такие как массовый сброс пароля или отключение Интернета

Менеджер инцидентов играет ключевую роль в процессе реагирования на инциденты, отвечая за оперативное управление, постановку задач и информирование об угрозах, а также за доведение основных проблем до руководства

C. Руководитель расследования

Руководитель расследования, как правило, старший специалист IR / Senior IT Operations, отвечает за проведение криминалистических расследований для понимания общего компромисса и информирования о связанных с ним рисках. Эта роль имеет решающее значение для определения масштаба, воздействия и первопричины инцидента, что определяет стратегию реагирования и помогает предотвратить подобные инциденты в будущем.

Ожидается, что представитель роли будет иметь серьёзное представление об ИТ-среде организации и ландшафте угроз. Представитель роли должен обладать навыками цифровой криминалистики и реагирования на инциденты (DFIR), а также уметь использовать различные инструменты и методы для анализа системных журналов, сетевого трафика и других данных для выявления признаков компрометации (IoC).

Представитель роли тесно сотрудничает с менеджером инцидентов, регулярно предоставляя обновлённую информацию о ходе расследования и его выводах, что имеет значение для поддержания прозрачности инцидента и понимания связанного с ним риска

В рамках роли может потребоваться сотрудничество с внешними организациями, например правоохранительными органами или сторонними поставщиками, особенно в случаях, связанных с юридическими вопросами или специализированной технической экспертизой

Представитель играет решающую роль в реагировании на инцидент в рамках своего технического опыта для понимания инцидента, разработки стратегии реагирования и информирования о риске менеджера инцидентов и руководителя управления.

D. Руководитель инфраструктуры

Эту роль обычно выполняет старший представитель по ИТ-операциям, который отвечает за сдерживание угрозы путём снижения риска, связанного с компрометацией.

Основная ответственность представителя роли заключается в сдерживании угроз — это принятие мер по ограничению распространения и воздействия инцидента безопасности в ИТ-инфраструктуре организации. Эта роль имеет решающее значение для управления техническими аспектами реагирования на инцидент и обеспечения эффективного сдерживания угрозы для предотвращения дальнейшего ущерба

Важность наличия выделенных ресурсов для каждой роли в структуре реагирования на инциденты означает, что лица, назначенные на эти роли, должны отдавать приоритет действиям по реагированию нежели другим задачам.

Что касается необходимых навыков, руководитель инфраструктуры должен обладать опытом, а также некоторыми знаниями в области операций по обеспечению безопасности, управления рисками и цифровой криминалистики. В документе представлена матрица навыков, в которой описываются требуемые и необязательные наборы навыков для каждой роли.

E. Менеджер по коммуникациям

Эта роль отвечает за контроль как внутренних, так и внешних сообщений кибербезопасности во время инцидента.

Специалист по коммуникациям является частью более крупной структуры реагирования на инциденты, которая включает в себя других руководителей.

Руководитель отдела коммуникаций, в частности, отвечает за взаимодействие с заинтересованными сторонами. Основная задача – контролировать обмен сообщениями как внешне, так и внутренне. Это включает в себя информирование о статусе и деталях инцидента соответствующих заинтересованных сторон внутри организации и за её пределами, обеспечивая распространение точной и своевременной информации. Это может помочь поддерживать доверие и предотвращать распространение дезинформации

Руководитель отдела коммуникаций также тесно сотрудничает с руководителем управления, который обеспечивает прозрачность и понимание рисков, связанных с инцидентом. Роль отвечает за оперативный надзор, обеспечение прозрачности ответных мер и понимание риска и воздействия на бизнес в целом.

F. Руководитель отдела регулирования

Эту роль обычно выполняет внутренний юрисконсульт или представитель по вопросам управления, рисков и комплаенса (GRC). Основными обязанностями являются проведение оценки рисков и воздействия, а также управление нормативными и правовыми требованиями для обеспечения соответствия во время инцидента в области кибербезопасности.

Роль имеет значение для обеспечения соответствия реакции организации на инцидент кибербезопасности законодательным и нормативным требованиям. Это может включать обязательства в соответствии с законами о защите данных, отраслевыми нормативными актами или договорными обязательствами. Роль также связана с поддержанием связи с регулирующими органами по мере необходимости и управление любыми юридическими последствиями инцидента.