УДК 004.056.5

КЛЮЧЕВЫЕ АСПЕКТЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО СОСТАВЛЕНИЮ ОТЧЕТА О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ ОРГАНИЗАЦИИ

Кропачев С.Ю.

преподаватель кафедры инфокоммуникационных и профессиональных дисциплин Волго-Вятского филиала Московского технического университета связи и информатики

Нижний Новгород, Россия

Аннотация

Данная статья исследует значимость и процесс составления отчетов о реагировании на инциденты информационной безопасности в современных организациях. Автор подробно рассматривает ключевые аспекты данного процесса, включая структуру отчета, используемые терминологию и методы анализа инцидентов. В статье также представлены методические рекомендации, направленные на повышение эффективности составления отчетов и улучшения процедур реагирования на угрозы информационной безопасности в корпоративной среде. Исследование выделяет важность правильного документирования инцидентов для обеспечения безопасности информационных систем и готовности организации к предотвращению будущих угроз.

Ключевые слова: угрозы информационной безопасности, инцидент информационной безопасности, отчет о реагировании, кибербезопасность.

KEY ASPECTS AND METHODOLOGICAL RECOMMENDATIONS FOR PREPARING A REPORT ON RESPONSE TO INFORMATION SECURITY INCIDENTS IN A MODERN ORGANIZATION

Kropachev S.Yu.

Lecturer of the Department of Infocommunication and Professional Disciplines, Volgo-Vyatsky Branch of the Moscow Technical University of Communications and Informatics

Nizhny Novgorod, Russia

Annotation

This article explores the importance and process of reporting information security incidents in modern organizations. The authors discuss in detail key aspects of this process, including report structure, terminology used, and incident analysis methods. The article also presents methodological recommendations aimed at increasing the efficiency of reporting and improving procedures for responding to information security threats in a corporate environment. The study highlights the importance of properly documenting incidents to ensure the security of information systems and the organization's preparedness to prevent future threats.

Keywords: information security threats, information security incident, response report, cyber security.

В современном цифровом мире, где угрозы информационной безопасности становятся все более сложными и разнообразными, а их реализация может привести к серьезным последствиям, таким как утечка конфиденциальных данных, нарушение целостности информации и нарушение работоспособности информационных систем. В данном контексте, отчет о реагировании на инцидент информационной безопасности является ключевым

инструментом не только для анализа произошедшего, но и для предотвращения подобных ситуаций в будущем. Необходимо отметить, что составление грамотного и качественного отчета о реагировании на инцидент информационной безопасности позволяет не только зафиксировать произошедшее событие, но и послужить основой для разработки дальнейших мер по укреплению информационной безопасности. Несомненно, что глубокий и детальный анализ инцидента позволяет выявить основные причины и уязвимости систем, подвергшихся воздействию, что в свою очередь способствует разработке эффективных стратегий предотвращения подобных инцидентов в будущем. В тоже время регулярное составление отчетов о реагировании на инцидент информационной безопасности также способствует формированию базы знаний, которая может быть использована для обучения персонала и улучшения информационной безопасности организации. Таким образом, отчет о реагировании на инцидент информационной безопасности является неотъемлемой частью процесса обеспечения информационной безопасности и играет важную роль в защите цифровых активов и данных.

В сфере обеспечения информационной безопасности важно понимать, что вопрос не заключается в том, случится ли инцидент безопасности вообще, а в том, когда он произойдет, поэтому для эффективного реагирования на угрозы информационной безопасности однозначно необходимы отчеты по реагированию на инциденты, которые будут служить связующим звеном между выявлением угроз и последующим их устранением. Отчеты по реагированию на инциденты информационной безопасности играют важную роль в архивировании прошлых инцидентов, являясь ценным источником уроков, извлеченных из предыдущих ошибок. Полученные знания могут быть легко интегрированы в общую стратегию предотвращения и смягчения будущих угроз информационной безопасности.

В целом, отчет по реагированию на инцидент информационной безопасности охватывает процесс, который организация реализует вследствие осуществления угрозы информационной безопасности. Его цель состоит в быстром выявлении атаки, минимизации ущерба, контроле и устранении причины для снижения риска будущих инцидентов и это имеет важное значение из-за нескольких ключевых причин. Во-первых, планы реагирования на инциденты критически важны, поскольку помогают ограничить и смягчить воздействия, причиняемые нарушением информационной безопасности. Это, в свою очередь, способствует управлению финансовым и репутационным ущербом организации, предоставляя при этом основу для предотвращения будущих инцидентов. В этом случае, отчеты по реагированию на инциденты играют решающую роль в том, чтобы специалисты по информационной безопасности могли последовательно реагировать на атаки и для составления такого эффективного отчета необходимо соблюдать баланс между техническими деталями и доступностью для понимания. Хороший отчет должен быть понятен как технической, так и непрофессиональной аудитории [2].

Хорошо составленный отчет по реагированию на инцидент информационной безопасности является инструментом для четкого понимания заинтересованными сторонами из различных сфер деятельности, включая юридические отделы, обеспечивающие соблюдение законодательства, руководство, оценивающее профили риска, и финансовых директоров, оценивающих финансовые последствия. Эта ясность полезна для всего процесса реагирования на инциденты, так как, во-первых, согласованные отчеты по реагированию на инцидент информационной безопасности позволяют специалистам изучить, как распознавать кибератаки на ранних стадиях, что способствует ее предотвращению или более быстрому восстановлению после отражения атаки. Во-вторых, позволяет минимизировать

продолжительность события и любые потенциальные отрицательные последствия. И в-третьих, многие регулирующие и сертификационные органы требуют, чтобы организации имели план реагирования на подобные инциденты.

В наиболее общем представлении организации могут быть подвержены угрозам различных видов атак, поэтому требуется системный подход к идентификации и классификации инцидентов информационной безопасности. Для быстрой идентификации инцидентов существуют три основных источника [4]:

- оповещение системы безопасности, среди которых можно выделить системы обнаружения вторжений (IDS/IPS), системы обнаружения и реагирования на инциденты (EDR/XDR), инструменты управления событиями и информационной безопасностью (SIEM) или даже простые оповещения антивирусов и данные NetFlow;

- обнаружение сотрудниками, например, пользователи могут замечать и сообщать о подозрительных действиях, необычных электронных письмах или аномальной работе систем;

- уведомления от третьих лиц, то есть партнеры, поставщики и даже клиенты также могут уведомлять организации об уязвимостях или нарушениях, с которыми они сталкиваются.

После идентификации инцидента информационной безопасности необходимо оперативно определить его категорию, так как это повлияет на его приоритет и выделение необходимых ресурсов. Среди распространенных типов инцидентов можно выделить вредоносное программное обеспечение (вирусы, черви, вымогательское ПО), фишинг, DDoS-атаки, несанкционированный доступ, утечку данных, физические проникновения.

После того как характер инцидента определен, сотрудники могут обращаться к планам реагирования на инциденты информационной

безопасности и, при необходимости, к предыдущим отчетам, чтобы понимать, какие действия необходимо предпринимать для устранения инцидента.

Важный аспект работы в области безопасности информации - это приоритизация инцидентов в зависимости от их серьезности, поэтому классифицируем инциденты по четырем уровням важности[1]:

1. Критический уровень - описывает неминуемые угрозы, которые могут подвергнуть опасности основные функциональные возможности бизнеса или чувствительные данные. Инциденты этого уровня требуют немедленного вмешательства для предотвращения серьезных последствий.

2. Высокий уровень - речь идет о возможных угрозах для бизнес-операций, которые, хотя и не немедленно разрушительны, имеют повышенный приоритет. Эти инциденты требуют быстрого вмешательства.

3. Средний уровень - инциденты этого уровня не создают неотвратимой угрозы для бизнес-операций, но требуют своевременного внимания для предотвращения ухудшения ситуации.

4. Низкий уровень - сюда относятся незначительные инциденты или какие-нибудь сетевые аномалии, которые могут быть управляемы в рамках стандартных операционных процессов информационной безопасности.

Таким образом, понимание и правильная оценка серьезности инцидентов позволяют эффективно распределять ресурсы и реагировать на угрозы в соответствии с их критичностью для бизнеса и его безопасности.

Следующим важным звеном является надежный процесс регистрации инцидентов, который будет служить единым каркасом для выявления, предотвращения и устранения нарушений информационной безопасности. В случае инцидента информационной безопасности можно следовать шаг за шагом следующему процессу регистрации:

1. Обнаружение инцидента. Несомненно, что прежде чем докладывать о инциденте, необходимо обнаружить и зафиксировать его наличие. Как уже

упоминали ранее инциденты информационной безопасности могут быть обнаружены с помощью инструментов, людей или третьей стороны.

2. Предварительный анализ. На этом этапе должен быть определен объем и потенциальные последствия инцидента информационной безопасности, проведя категорирование на основе ранее установленных классификаций и метрик серьезности инцидента.

3. Регистрация инцидента. Предполагается, что каждое действие и наблюдение, связанное с инцидентом безопасности, должно быть тщательно зарегистрировано с использованием имеющейся системы контроля, так, например, популярными платформами для этой цели являются система JIRA и проект TheHive.

Вне зависимости от степени серьезности об инциденте информационной безопасности должны быть уведомлены все заинтересованные стороны, которые можно разделить на две группы:

- соответствующие внутренние отделы, такие как ИТ, юридический, связи с общественностью и исполнительные команды, при этом в случаях, когда инцидент имеет широкие и серьезные последствия, может потребоваться уведомление всей организации.

- в зависимости от характера, серьезности и тяжести последствий инцидента, может потребоваться уведомление клиентов, партнеров, регулирующих органов или даже широкой публики.

Для понимания полного воздействия инцидента необходимо провести детальное внутреннее расследование, ключевым этапом которого является комплексный технический анализ в сочетании с сбором всех результатов. Продолжительность такого глубокого расследования может значительно варьироваться, от нескольких дней до потенциально нескольких лет.

Итогом работы аналитика или специалиста информационной безопасности является создание завершенного отчета о реагировании на

инцидент информационной безопасности, который предоставит регулирующим органам, страховым компаниям и руководству организации подробное описание инцидента информационной безопасности, его происхождение и принятые меры по устранению.

Далее рассмотрим важные составляющие отчета о реагировании на инцидент информационной безопасности, которые обязательно должны быть отражены в результирующем документе.

Вступительная часть отчета, как правило, предназначается для широкой аудитории, поэтому рекомендуется избегать слишком многих технических деталей, принимая во внимание главную цель этого раздела - предоставить краткий обзор инцидента, основные выводы, принятые немедленные меры и влияние на заинтересованные стороны. Необходимо обязательно присвоить и указать уникальный идентификатор инцидента, чтобы можно было в дальнейшем оптимизировать и организовать работу с архивами. В кратком изложении событий инцидента указать его тип, согласно ранее приведенной квалификации, времени совершения и даты инцидента, его продолжительность, затронутые информационные системы (данные) и текущий статус. В основных выводах перечислить полученные результаты инцидента, ответив на следующие вопросы. Какова была основная причина инцидента? Была ли использована конкретная уязвимость CVE? Какие данные, если таковые имеются, были скомпрометированы, извлечены или подверглись опасности? Были ли затронутые системы немедленно изолированы? Привлекались ли сторонние службы, и если да, то какие? По возможности оценить потенциальное воздействие на различные заинтересованные стороны. Например, испытывали ли клиенты простои, и каковы финансовые последствия? Были ли скомпрометированы данные сотрудников?

Далее идет раздел технического анализа, в котором детальнее описывается техническая сторона произошедшего инцидента информационной

безопасности. Это самая обширная часть отчета об инциденте, которая должна включать в себя следующее:

- скомпрометированные системы и данные, то есть всё, что было либо потенциально доступно, либо точно скомпрометировано во время инцидента;

- источники цифровых следов и доказательств, примененные методы анализа и их результаты;

- выявленные показатели компрометации (Indicator of Compromise, IOC), которые позволяют отнести реализованную атаку к конкретной группе угроз;

- подробное описание основной причины инцидента информационной безопасности (использованные уязвимости, точки отказа и т. д.), полученные в результате анализ основной причины инцидента;

- построенная хронология событий, так как очень важно понять последовательность действий нарушителя, включая первоначальное проникновение, перемещение по сегменту локальной сети, доступ к данным, время его обнаружения и изоляции, время блокирования дальнейшего развития инцидента и время, затраченное на восстановление;

- провести анализ характера атаки, ее тип, тактики, техники и процедуры (TTPs), использованные злоумышленником.

Далее необходимо определить и оценить влияние негативных последствий, которые произошли в результате инцидента информационной безопасности на данные, операции и репутацию организации. В первую очередь, при наличии такой возможности, составить и определить количественное измерение ущерба, причиненного инцидентом, опираясь на то, что уже предварительно установили какие именно системы, процессы или наборы данных были скомпрометированы. Также оценить потенциальные последствия для деятельности организации, такие как финансовые потери, штрафы по регулятивным нормам и ущерб репутации.

В следующей части отчета освещаются конкретные меры, принятые для ограничения инцидента информационной безопасности, ликвидации угрозы и восстановления нормальной работы подвергшихся воздействию систем.

В первую очередь, описываются мероприятия, которые были предприняты сразу же после обнаружения инцидента информационной безопасности. Как правило — это определение скомпрометированных учетных записей и затронутых систем, включая подробное описание методов и инструментов, использованных для определения компрометации, а также подробное описание технических методов, использованных для прекращения доступа, таких как блокировка учетных записей, изменение разрешений или изменение правил брандмауэра. Необходимо установить время обнаружения несанкционированного доступа, с точностью до минут, если это возможно. По окончании выполнения мероприятий следует подтвердить воздействие принятых мер, оценить то, что насколько они достигли цели, включая предотвращение эксфильтрации данных или дальнейшей компрометации систем.

Во вторую очередь, целесообразно указать меры по недопущению распространения инцидента, разделив их на следующие периоды

1. В краткосрочном периоде - немедленные меры по изоляции подвергшихся воздействию систем от локальной сети организации для предотвращения внутреннего перемещения злоумышленника.

2. В долговременной перспективе – более глобальные меры, например, такие как сегментация локальной сети организации или реализация архитектуры нулевого доверия (zero-trust).

Аналогично завершению предыдущего этапа, необходимо проверить эффективность принятых мер, то есть оценить результативность проведенных мероприятий посредством анализа последствий, причиненных инцидентом информационной безопасности.

В-третьих, подробно описываются меры, непосредственно принятые для ликвидации инцидента. Если злоумышленниками использовалось вредоносное программное обеспечение, то нужно указать применяемые способы его обнаружения, включая детектирование конкретными средствами обнаружения и реагирования как на конечных точках (EDR), так и в системе в целом (IDS, IPS), дополнительно перечислить конкретные программные продукты, применяемые для удаления вредоносного программного обеспечения, и методы их использования. Обязательно отразить верификацию выполненных мероприятий, то есть проверить их эффективность по обнаружению, нейтрализации и полному устранению вредоносного программного обеспечения.

В-четвертых, перечисляются меры, принятые по выявлению и устранению уязвимостей подвергшихся воздействию систем. Для этого необходимо проанализировать какими именно дефектами и уязвимостями воспользовались злоумышленники, с помощью каких средств были обнаружены эти уязвимости, включая определение идентификаторов CVE, если это общеизвестные и доступные уязвимости. По результатам ликвидации составить подробное описание самого процесса устранения уязвимостей, включая этапы тестирования, развертывания исправлений и обновлений безопасности и последующему подтверждению результативности принятых мер. Обязательно предусмотреть вероятность нестабильной работы систем после применения исправлений и обновлений безопасности и разработать мероприятия, которые необходимо будет реализовать для их отмены и возвращения к нормальному функционированию.

В-пятых, подробно описать мероприятия по восстановлению данных из резервных копий, при этом необходимо отдельно указать методы дешифрования, используемые в том случае, если перед хранением данные были зашифрованы. Рекомендуется предусмотреть проверку работоспособности

резервных копий перед их развертыванием, для этого заранее определить и апробировать процедуры для проверки целостности резервных копий перед их восстановлением и обязательно указать методы, применяемые для проверки целостности восстановленных данных и их верификации.

На заключительном этапе этого раздела необходимо выделить действия, предпринимаемые для обеспечения безопасности систем перед их повторным запуском, например, такие как перенастройка межсетевых экранов или обновление систем обнаружения вторжений (IDS), а также разработать и перечислить мероприятия, которые включают в себя тесты, проводимые для подтверждения того, что системы полностью функциональны и работают требуемым образом в производственной среде.

После локализации, нейтрализации и устранения последствий инцидента в отчете необходимо указать мероприятия, которые не позволят в дальнейшем допустить аналогичный инцидент информационной безопасности. Например, составить планы усиленного мониторинга, то есть подробные планы для непрерывного мониторинга с целью выявления аналогичных уязвимостей или шаблонов атак в будущем. В дополнение к таким планам определить и указать конкретные средства мониторинга, которые будут использоваться, и как они интегрируются с существующими системами для комплексного обзора.

По результатам проведенного расследования инцидента информационной безопасности необходимо провести тщательную оценку не сработавших должным образом мер безопасности и причин их возникновения, составить рекомендации на основе извлеченных уроков, разбитые по приоритетам и временным рамкам для реализации и определить долгосрочные изменения в политике, архитектуре или обучении персонала для предотвращения аналогичных инцидентов.

В приложениях к отчету можно разместить дополнительные материалы, который предоставляют дополнительный контекст, доказательства или

технические детали, критически важные для полного понимания инцидента информационной безопасности, его последствий и принятых мер реагирования. Несмотря на то, что это последняя часть отчета о реагировании на инцидент, это тоже важное звено в структуре отчета, поскольку приложения придают убедительность и глубину смысловому наполнению, представленному в основной части отчета.

В этом разделе могут быть включены следующие элементы:

- лог-файлы;
- сетевые диаграммы (до инцидента и после инцидента);
- следственные доказательства (образы дисков, дампы памяти и пр.);
- фрагменты кода;
- контрольный список (чеклист) реагирования на инцидент;
- документы о коммуникациях;
- юридические и регуляторные документы (формы соответствия, NDA, подписанные внешними консультантами и пр.);
- словарь терминов.

Подводя итоги, на основании вышеизложенного сформировали оптимальную структуру отчета о реагировании на инциденты информационной безопасности, и в заключение необходимо указать некоторые ключевые моменты, на которые следует всегда обращать внимание.

Во-первых, всегда старайтесь найти основную причину инцидента, чтобы предотвратить его возникновение в будущем. При анализе основной причины инцидента, аналитик или специалист по информационной безопасности должен использовать различные методы, включая техники отслеживания, анализа журналов событий и проверки кода приложений.

Во-вторых, обменивайтесь нечувствительными для организации подробностями с профильными сообществами специалистов по

информационной безопасности для повышения коллективной кибербезопасности.

И в-третьих, регулярно информируйте все заинтересованные стороны на протяжении всего процесса реагирования на инцидент, например, составляйте отчеты о текущем состоянии, изменениях в процессе реагирования и планах действий.

При наличии возможности, рассмотрите привлечение сторонних специалистов по кибербезопасности для проверки результатов и эффективности реагирования на инцидент. Внешние эксперты проводят независимую оценку методов и результатов реагирования на инциденты, что способствует повышению эффективности и надежности процесса обеспечения кибербезопасности.

Библиографический список:

1. Information Security Handbook by Darren Death, Released December 2017 Publisher(s): Packt Publishing, 330 pages URL - https://freecomputerbooks.com/The-Information-Security-Handbook.html

2. Джейсон А. Защита данных. От авторизации до аудита. — СПб.: Питер, 2021. — 272 с.

3. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства : учебное пособие / В. В. Бондарев. — Москва : Издательство МГТУ им. Н. Э. Баумана, 2017. — 225 с.

4/ Прохорова О. В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург : Лань, 2022. — 124 с.

4. Информационная безопасность цифрового пространства / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб. : Изд-во СПбГЭУ, 2019. – 155 с.

5. Энсон С. Реагирование на компьютерные инциденты. Прикладной курс / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2021. – 436 с.

Оригинальность 85%