Шаханова М. В., Лутов Е. В., Шаханова Э. С. Выявление событий информационной безопасности с помощью индикаторов компрометации // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 59–64

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ВЫЯВЛЕНИЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ ИНДИКАТОРОВ КОМПРОМЕТАЦИИ

Шаханова М. В., Лутов Е. В., Шаханова Э. С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

Настоящая статья посвящена вопросам, раскрывающим роль индикаторов компрометации, позволяющих предупреждать события информационной безопасности, повысить надежность и информационную безопасность информационной системы предприятия. В статье также рассказывается о необходимости интеграции имеющихся индикаторов в существующие системы слежения и управления информационной безопасностью.

Ключевые слова. Индикатор компрометации, инцидент информационной безопасности, система менеджмента инцидентами информационной безопасности, интеграция, защита данных.

IDENTIFICATION OF INFORMATION SECURITY EVENTS USING INDICATORS OF COMPROMISE

Shakhanova M. V., Lutov E. V., Shakhanova E.S.
G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

This article is devoted to issues that reveal the role of indicators of compromise, allowing to prevent information security events, improve the reliability and information security of an enterprise information system. The article also talks about the need to integrate existing indicators into existing tracking and information security management systems.

Keywords: Indicator of compromise, information security incident, information security incident management system, integration, data protection

Вмешательство человека в информационное пространство предприятий может оказать существенное влияние на структуру информационной безопасности, вызвать нежелательные события и инциденты. Вмешательство человека может быть случайным и преднамеренным. В последнем случае, как правило, преследуются корыстные интересы, наносится большой вред организации. По данным исследовательского отчета института Ponemon, подсчитанный примерный ущерб от атак на информационные системы розничных магазинов за период только с 2019 по 2020 гг. вырос с 8 млн. $ и превысил значение в 12 млн. $ на каждое большое предприятие. Среди финансовых организаций средний ущерб превышал двадцать млн. $, в технологическом секторе – свыше четырнадцати млн. $, в среднем на одно предприятие [5].

Важно контролировать все попытки вмешательства и структуру информационной системы предприятия, иметь для этого соответствующие средства, которые бы регистрировали все события (инциденты) информационной безопасности, предоставляли бы удобные средства консолидации данных для анализа уязвимостей информационной системы предприятия. Такие средства позволят предупреждать события информационной безопасности, повысить надежности и информационную безопасность технологического сегмента предприятия.

Информация в окружающем мире представляет сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления [1]. Для того, чтобы информация, которой оперируют сотрудники в процессе своей деятельности, была пригодной, она должна обладать следующими качествами [2]:

- объективность и субъективность;
- полнота – содержать необходимое и достаточное количество фактов для принятия решения;
- достоверность – соответствовать объективной модели реальности в текущем контексте;
- адекватность – объективная оценка достоверности информации в соответствии с принятым контекстом;
- доступность информации – уровень защиты источников и доступа к информации;
- актуальность – показатели таких характеристик, как достоверность и адекватность относительно настоящего момента времени;
- репрезентативность – уровень отбора свойств информации для представления и описания интересующего объекта / явления / процесса;
- содержательность – отношение количества семантической информации в сообщении к объему обрабатываемых данных;
- точность – характеристика меры схожесть информации с описанием реального объекта / явления / процесса;
- устойчивость – показатель модифицируемости выходных данных в качестве отклика на изменение входных данных;
- преобразуемость – показатель вариативности представления информации в зависимости от контекста.

Важно иметь подробную классификацию угроз ИБ, чтобы в каждом конкретном случае возникающую угрозу можно было соотнести с известным классом и оценить возможное влияние последствий в соответствии с базовыми параметрами, описанными в классе (наработанными в результате опыта). Анализ массива данных по угрозам ИБ по классам позволит систематизировать основные характеристики угроз ИБ и тем самым может способствовать разработке превентивных мер, мер по устранению последствий и т.д.

Так, на Рисунке 1 приведены наиболее опасные угрозы ИБ по данным опроса, проведенного в рамках исследования «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция» [5].

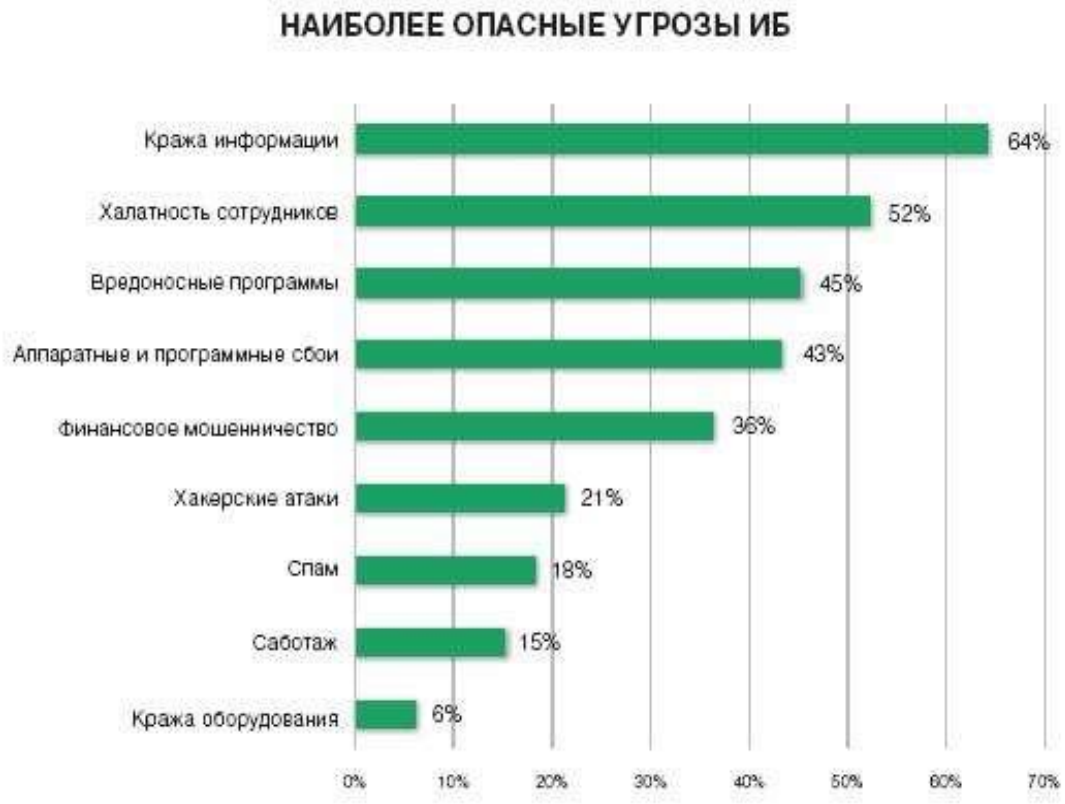

Рисунок 1 – Наиболее опасные угрозы ИБ [5, 2021 г.]

Почти в каждом случае инцидент информационной безопасности не приходит одномоментно. Почти всегда этому предшествуют сопутствующие действия, связанные с выявлением уязвимостей, хищением секретных ключей и т.д. Это, например, шпионаж, социальная инженерия, внедрение троянских программ в инфраструктуру и т.д. Множество таких подготовительных действий злоумышленников можно попытаться распознать на ранних этапах попыток компрометации системы информационной безопасности. Для этого главную роль играют специальные индикаторы компрометации.

Индикаторы компрометации в своем многообразии представляют собой различные методы и средства:

- организационные;
- программно-технические;
- технологические.

Организационные меры обеспечивают документальную и методическую поддержку функционирования индикаторов компрометации. К ним относятся документация на комплексы (например, руководство пользователя), политика информационной безопасности, должностная инструкция службы безопасности. В этих документах должны быть четко прописаны характеристики индикаторов, правила работы с ними, комплекс мероприятий, проводимых для предупреждения, выявления, реакции и последующего устранения угроз информационной безопасности. Таким образом, организационное обеспечение индикаторов компрометации устанавливает правила их использования, а, часто еще устанавливает формы отчетности и протоколы ведения журнала регистрации событий.

Программно-технические средства индикаторов компрометации являются основными рабочими схемами в системе обеспечения информационной безопасности. Так, в их состав входят:

- аппаратные брандмауэры и сетевые экраны, в «прошивку» которых входят функции обнаружения подозрительных абонентов;
- сетевая коммутационная аппаратура с интеллектуальными алгоритмами распознавания попыток вторжения, например, через заблокированные порты;
- системы контроля и управления доступом (СКУД), сигнализирующие о попытках несанкционированного доступа;
- специальное программное обеспечение, отслеживающее подозрительные файлы на компьютерах (например, антивирусы);
- специальное программное обеспечение, контролирующее содержимое трафика сети и сигнализирующее о попытках передачи подозрительных данных и / или попытках высоко загрузить сеть (сервер);
- протоколы, действующие в сети, позволяющие идентифицировать и аутентифицировать цифровые подписи, содержимое электронных писем, электронных сертификатов.

Все эти средства должны работать в комплексе и быть объединены общей базой данных, в которую будут записываться все события, регистрируемые индикаторами.

Назначение индикаторов компрометации системы информационной безопасности состоит в регистрации всех подозрительных событий и попыток несанкционированного вторжения в информационную инфраструктуру. При этом для наиболее эффективного практического применения индикаторов необходимо иметь специальную систему, работающую над всеми индикаторами. Такую систему часто называют системой менеджмента инцидентов информационной безопасности [3]. В рамках такой системы необходима реализация следующих функций:

- ведение базы знаний (справочника) типов инцидентов, их приоритета, оценок критичности, признаков, оценок последствий и т.д.;
- автоматическая классификация всех регистрируемых индикаторами событий в соответствии с группами, выделенными в базе знаний;
- построение аналитических отчетов в виде таблиц, графиков и диаграмм, наглядно показывающих состояние мониторинга безопасности информационных систем предприятия; при этом необходима возможность анализа всех зарегистрированных инцидентов с помощью агрегирующих функций (например, группировка по узлам системы, типам событий, адресам / источникам и т.д.).

Правильное применение системы управления инцидентов информационной безопасности, зарегистрированных индикаторами, позволит прогнозировать, предотвращать и снижать риск повторных компрометаций, найти слабые и уязвимые места в системе ИБ. При этом система управления инцидентов информационной безопасности должна основываться на следующих прецедентах [4]:

- идентификация (система управления);
- сигнализация (индикаторы);
- регистрация (индикаторы);

- выявление причин, оценка влияния, устранение последствий, внесение изменений для устранения причин (анализ и решения);
- разработка превентивных мер (анализ и решения);
- расследование (анализ и решения);
- анализ данных и принятие управленческих решений (анализ и решения).

На Рисунке 2 приведена схема жизненного цикла события компрометации (инцидента), зарегистрированного индикатором, приведенная в руководстве по реагированию от лаборатории Касперского [6].

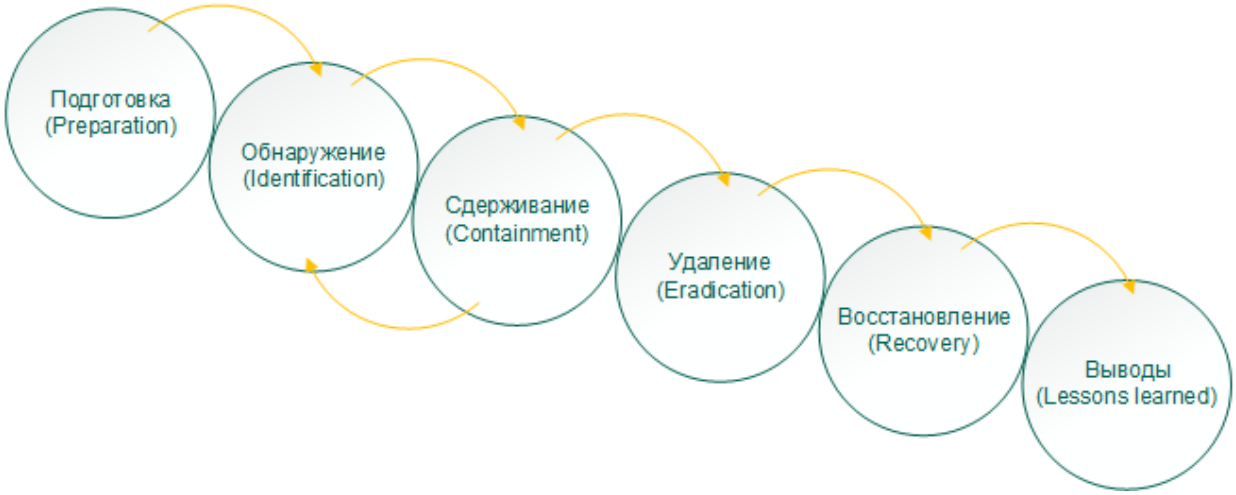

Рисунок 2 – Этапы управления инцидентом информационной безопасности

Выполнение приведенных на рисунке этапов управления инцидентами информационной безопасности подразумевает интеграцию индикаторов компрометации в систему управления инцидентами, базу знаний, базу данных, специального пакета программного обеспечения, форм ввода данных и форм итоговых документов. Поэтому можно сформировать следующие требования к системе, в которой должны функционировать индикаторы компрометации системы ИБ:

- наличие контролирующей службы ИТ-подразделения, выполняющей слежение за соблюдение политики ИБ на предприятии;
- интеграция специального модуля регистрации инцидентов ИБ;
- ведение базы знаний по видам, типам, характеристикам, признакам и превентивным мерам инцидентов;
- интеграция с экспертной системой, которая будет идентифицировать инциденты и предлагать варианты решения из базы знаний;
- стандартизация индикаторов (как минимум, стандартизация протоколов, по которым будут записываться в хранилище данных зарегистрированные события);
- разработка организационного обеспечения, включающего документы по использованию базы знаний, экспертной системы и индикаторов;
- обеспечение безопасности сетевой инфраструктуры;
- внедрение прикладного программного обеспечения системы менеджмента инцидентов информационной безопасности, интегрированного с экспертной системой, базой знаний и индикаторами.

Список литературы

1. ГОСТ Р 56546-2015. Уязвимости информационных систем п. 3.1
2. ГОСТ Р 56546-2015. Уязвимости информационных систем п. 3.5
3. ГОСТ Р ИСО/МЭК 18044 – 2007. Менеджмент инцидентов информационной безопасности
4. ГОСТ Р ИСО/МЭК 27001 – 2006. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности, ст. 3.6
5. Международное исследование EY в области информационной безопасности «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция» // 2021 г.
6. Руководство по реагированию на инциденты информационной безопасности // Управление технологических решений // АО Kaspersky Lab., – Версия 1.0 (07.03.2022)

References

1. GOST R 56546-2015. Vulnerabilities of information systems p. 3.1
2. GOST R 56546-2015. Vulnerabilities of information systems p. 3.5
3. GOST R ISO / IEC 18044 - 2007. Management of information security incidents
4. GOST R ISO / IEC 27001 - 2006. Information technology (IT). Methods and means of ensuring security. Information security management systems, art. 3.6
5. EY international study in the field of information security "The path to cyber resilience: forecast, resistance, response" // 2021
6. Guidelines for responding to information security incidents // Management of technological solutions // AO Kaspersky Lab., - Version 1.0 (03/07/2022)