Международный союз электросвязи

МСЭ-Т X.1216

(09/2020)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Кибербезопасность

Требования к сбору и сохранению доказательств инцидентов кибербезопасности

Рекомендация МСЭ-Т X.1216

ITU-T

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	**X.1200–X.1229**
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1379
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1216

Требования к сбору и сохранению доказательств инцидентов кибербезопасности

Резюме

В Рекомендации МСЭ-Т X.1216 описана общая процедура реагирования на инциденты кибербезопасности и расследования инцидентов кибербезопасности. Проведен анализ источников доказательств инцидентов кибербезопасности и определены требования к возможностям инструментов, используемых для сбора и сохранения таких доказательств в процессе расследования. В настоящей Рекомендации определены также требования гарантии надежности этих инструментов в форме руководства для разработчиков, проектирующих инструменты для этих целей.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1216	03.09.2020 г.	17-я	11.1002/1000/14259

Ключевые слова

Кибербезопасность, доказательства инцидентов кибербезопасности, реагирование на инциденты и расследование инцидентов.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например: http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1216

Требования к сбору и сохранению доказательств инцидентов кибербезопасности

1 Сфера применения

В настоящей Рекомендации описана общая процедура реагирования на инциденты кибербезопасности и расследования инцидентов кибербезопасности. Кроме того, проведен анализ источников доказательств инцидентов кибербезопасности и определены требования к возможностям инструментов, используемых для сбора и сохранения таких доказательств в процессе расследования. В настоящей Рекомендации определены также требования гарантии надежности этих инструментов в форме руководства для разработчиков, проектирующих инструменты для этих целей.

В настоящей Рекомендации не рассматриваются вопросы конфиденциальности и положения, относящиеся к сбору данных об инцидентах кибербезопасности, судебным разбирательствам, дисциплинарным процедурам и другим соответствующим действиям при работе с потенциальными доказательствами инцидентов кибербезопасности. Эти элементы считаются выходящими за рамки "сбора и сохранения".

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 сбор (collection) [b-ISO/IEC 27037]: Процесс сбора физических элементов, которые содержат потенциальные свидетельства в цифровой форме.

3.1.2 доказательство (evidence) [b-ITU-T X.813]: Информация, которая сама по себе или в сочетании с другой информацией может использоваться для разрешения спора.

3.1.3 расследование (investigation) [b-ISO/IEC 27042]: Применение экспертизы, анализа и интерпретации для содействия в понимании инцидента.

3.1.4 сохранение (preservation) [b-ITU-R BR.1351]: Операции технического обслуживания, которые необходимо выполнить для обеспечения надлежащего сохранения архивных материалов, такие как периодическая проверка степени ухудшения состояния носителей и, при необходимости, восстановление контента на новых носителях.

3.1.5 инцидент безопасности (security incident) [b-ITU-T E.409], [b-IETF RFC 2828]: Любое неблагоприятное событие, которое может создать угрозу для определенного аспекта безопасности.

3.1.6 метка времени (timestamp) [b-ISO/IEC 27037]: Изменяющийся во времени параметр, который обозначает момент времени в привязке к единому времени.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 доказательства инцидентов кибербезопасности (cybersecurity incident evidence): Информация или данные, хранящиеся или передаваемые в двоичной форме, которые в процессе анализа были определены как имеющие отношение к расследованию инцидента кибербезопасности.

ПРИМЕЧАНИЕ. – Это определение основано на определении "цифровое доказательство" в ISO/IEC 27037.

3.2.2 защита с использованием движущихся целей (moving target defence): Механизмы, автоматически изменяющие один или несколько атрибутов системы, для того чтобы сделать область атаки системы непредсказуемой для злоумышленников.

ПРИМЕЧАНИЕ. – Это определение основано на [b-Jajodia14].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения.

ARP	Address Resolution Protocol	Протокол разрешения адресов
BYOD	Bring Your Own Device	Принеси свое собственное устройство
DLL	Dynamic Linked Library	Библиотека динамической компоновки
IP	Internet Protocol	Протокол Интернет
MAC	Media Access Control	Управление доступом к среде передачи
MTD	Moving Target Defence	Защита с использованием движущихся целей
PE File	Portable Executable File	Переносимый исполняемый файл
PII	Personally Identifiable Information	Информация, позволяющая установить личность
WORM	Write Once Read Many	Однократная запись, многократное чтение

5 Соглашения

В настоящей Рекомендации:

ключевые слова "**требуется**, **чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящему документу;

ключевое слово "**следует**" или "**должен**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии это требование не является обязательным.

6 Обзор доказательств инцидентов кибербезопасности

6.1 Общая процедура реагирования на инциденты и их расследования

При анализе причин инцидента кибербезопасности критически важным компонентом реагирования и расследования является сбор и сохранение доказательств, связанных с этим инцидентом, поскольку проанализированные данные об инциденте кибербезопасности могут стать потенциальными свидетельствами в судебных разбирательствах. Кроме того, собранные доказательства инцидента кибербезопасности могут быть использованы для изучения уязвимостей организации в целях повышения уровня ее кибербезопасности.

Процедура расследования инцидента, показанная на рисунке 1, состоит из следующих последовательных этапов.

– Подготовка – на этом этапе следует провести предварительную подготовку к расследованию инцидента.

– Обнаружение – на этом этапе устанавливается факт несанкционированного события, то есть инцидента. В зависимости от серьезности инцидента, помимо сбора данных, следует принять решение о порядке реагирования на это событие.

– Сбор данных – данные следует получать от инструментов, используемых для сбора данных о трафике. Этот этап очень важен. Обмен данными о трафике осуществляется с высокой скоростью, поэтому позднее получить те же данные о сетевом трафике будет невозможно.

– Сохранение данных – полученные исходные данные о сетевом трафике следует сохранять на устройстве резервного копирования, сохраняется также хеш-код всех данных.

– Расследование – на этом этапе следует свести вместе все собранные следы. Производится поиск доказательств для выявления артефактов атаки. Признаки классифицируются и сопоставляются и на их основе выполняются важные наблюдения с использованием существующих атак. На этом этапе может быть установлен тракт атаки, и путем многократного выполнения анализа атрибутов можно прийти к заключению в отношении идентификационных данных злоумышленника.

– Отчет – наблюдения и пояснения к расследованию следует излагать языком, понятным юристам.

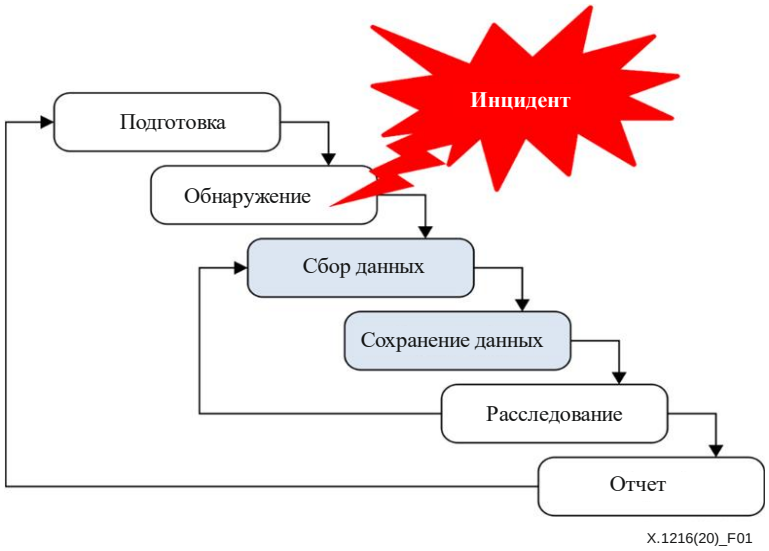

Рисунок 1 − Общая процедура расследования инцидента

Различные руководящие указания ИСО/МЭК, относящиеся к цифровому расследованию и реагированию на инциденты, стандартизированы в документах [b-ISO/IEC 27035-3], [b-ISO/IEC 27037], [b-ISO/IEC 27041], [b-ISO/IEC 27042] и [b-ISO/IEC 27043]. Эти руководящие указания предназначены в основном для предоставления информации о передовом опыте и обработки цифровых доказательств на всех этапах процедуры расследования инцидентов. В [b-IETF RFC 3227] также содержатся руководящие указания по сбору и архивированию доказательств, включая подготовку и рассмотрение этапов сбора данных; выбор архивных носителей и документации для обеспечения сохранности вещественных доказательств при их передаче; набор инструментов, необходимых для сбора и архивирования доказательств. Однако руководящие указания по выбору или разработке инструментов расследования сформулированы недостаточно четко.

6.2 Источники данных об инцидентах кибербезопасности

Типичными источниками данных, относящихся к инцидентам кибербезопасности, являются хост-устройства, устройства обеспечения сетевой безопасности, сетевые устройства и сети. На рисунке 2 представлена классифицированная информация, получаемая от источников данных.

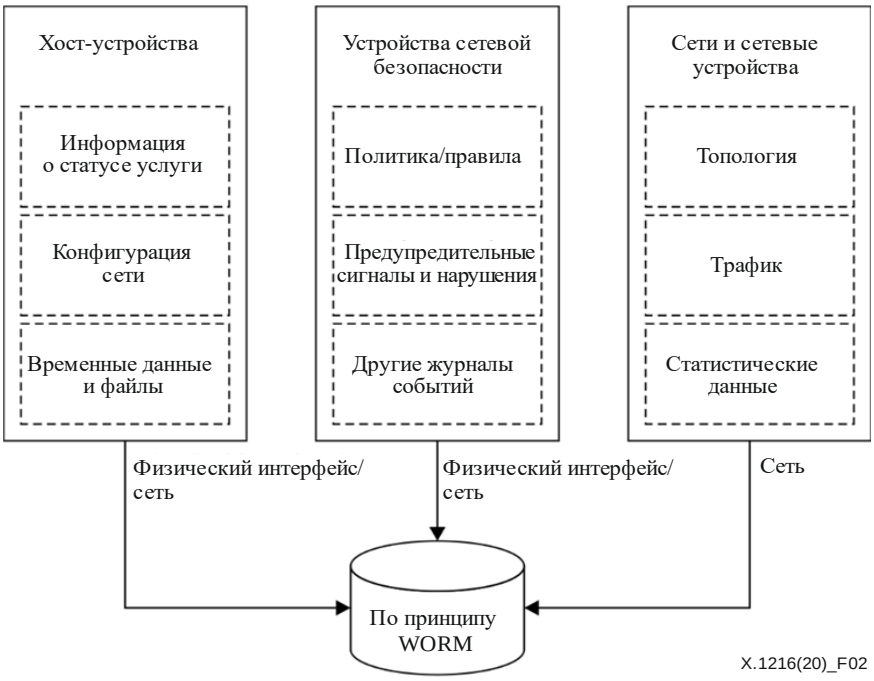

Рисунок 2 − Различные источники данных об инцидентах кибербезопасности

6.2.1 Хост-устройства

Как правило, хост-устройство предоставляет различные виды данных, относящихся к инцидентам кибербезопасности. Следует, чтобы инструменты сбора данных тщательно собирали эти данные, поскольку некоторые из них нестабильны и могут быть легко уничтожены. С хост-устройства можно собрать данные следующих типов.

1) Сведения, относящиеся к состоянию системы:
   - общие сведения (имя хоста, информация об учетной записи пользователя, системные дата и время, время последней загрузки, текущий часовой пояс, загрузочное устройство);
   - сведения об операционной системе (производитель, название, архитектура, версия, серийный номер, дата установки);
   - прикладные программы (установленные программы, статус исправлений, переменные среды);
   - процессы (таблица процессов, автоматически запущенные процессы, плановые служебные процессы);
   - сеанс входа в систему;
   - другие данные регистра.
2) Сведения, относящиеся к данным и устройствам хранения:
   - данные запоминающего устройства;
   - временные файловые системы (недавно использовавшиеся или выполнявшиеся файлы, включая библиотеку динамической компоновки (DLL) и дескрипторы);
   - скрытые файлы, исполняемые файлы, открытые файлы, удаленные файлы, нераспределенная область;
   - архивные носители;
   - совместно используемые данные (общие папки, сетевые устройства).

3) Сведения, относящиеся к организации сети:

– таблица маршрутизации, кеш протокола разрешения адресов (ARP0, статистика ядра;
– сетевые конфигурации (IP-адреса, адреса управления доступом к среде передачи (MAC), открытые порты, сетевые интерфейсы);
– сведения, относящиеся к интернет-браузеру (история интернет-браузера, недавно посещенные интернет-объекты, cookie-файлы).

6.2.2 Устройства сетевой безопасности

Данные, относящиеся к атаке, следует собрать от устройств сетевой безопасности, таких как системы обнаружения проникновений и брандмауэры:

– политика безопасности (контроль доступа, правила обнаружения);
– события, связанные с безопасностью, и журналы таких событий (предупредительные сигналы, аварийные сигналы, уведомления, сообщения об ошибках);
– статистические данные.

6.2.3 Сети и сетевые устройства

При расследовании кибератак важно собрать данные от сетей. В частности, при расследовании киберинцидентов информация о топологии сети помогает изучить компоненты и конфигурации сети предприятия, выявить тракты атаки и оценить степень ущерба. Это особенно важно в наши дни, когда конфигурация сети изменяется динамически вследствие использования облачных вычислений, виртуальных машин и таких методов, как "принеси свое собственное устройство" (BYOD) и "защита с использованием движущихся целей" (MTD). Типичными примерами данных о сети и сетевых устройствах являются:

– конфигурация топологии сети;
– журналы событий маршрутизатора;
– сетевые услуги;
– информация о подключенных к сети хост-устройствах (открытые порты, внутренние услуги по эксплуатации, состояние);
– следы трафика, включая заголовок и данные;
– сведения о потоке данных сеанса (IP-адрес/номер порта источника, IP-адрес/номер порта назначения, протокол, другая информация заголовков TCP);
– файлы, передаваемые по сети;
– статистика сетевого трафика.

7 Требования к сбору данных об инцидентах кибербезопасности

Не менее важным, чем решение о выборе данных, которые необходимо собирать в случае инцидента кибербезопасности, является решение о том, каким образом собирать, сохранять и анализировать эти данные. В данном разделе описываются возможности по сбору данных об инциденте кибербезопасности из источников данных трех типов, представленных в разделе 6.

Сведения из журналов регистрации и другие данные об инциденте, собранные из источников данных, могут содержать информацию, позволяющую установить личность (PII). Исполнителям следует минимизировать сбор любой PII, оставив лишь то, что абсолютно необходимо для составления отчета об инциденте и реагировании на него, и защищать PII в соответствии с надлежащими и применимыми законами и правилами.

7.1 Сбор данных об инцидентах кибербезопасности от хост-устройств

Хост-устройства обычно служат основным источником данных для анализа инцидентов кибербезопасности. Они предоставляют данные, относящиеся к системным регистрам, журналам событий и файлам, загруженным системой. Когда требуется более точный анализ, следует получить дамп памяти хост-устройства.

Для этого инструмент сбора данных должен обеспечивать следующие возможности:

– исследование процессов и сбор информации о процессах;
– сбор данных о состоянии системы;
– выполнение побитового копирования;
– генерирование образов ядра;
– автоматизацию процессов сбора данных;
– импорт и экспорт собранных данных;
– поддержку различных операционных систем хост-устройств;
– предоставление библиотек, необходимых для сбора данных, без использования каких-бы то ни было библиотек на хост-устройствах;
– сбор непостоянных данных во время работы системы; и
– сбор данных о сетевом состоянии текущего соединения и открытого сокета.

7.2 Сбор данных об инцидентах кибербезопасности от устройств сетевой безопасности

Большое количество данных, полезных для анализа инцидентов кибербезопасности, можно получить от устройств сетевой безопасности, таких как системы защиты от проникновений, системы обнаружения проникновений, системы предотвращения проникновений, системы сетевой защиты, системы управления информацией о безопасности и администрирования событий.

Для обеспечения этого инструмент сбора данных должен обладать следующими возможностями:

– сбор журналов событий от устройств сетевой безопасности;
– сбор журналов предупреждений и нарушений от устройств сетевой безопасности;
– сбор журналов аутентификации пользователей от устройств сетевой безопасности;
– сбор информации о политике и правилах безопасности устройств сетевой безопасности.

7.3 Сбор данных об инцидентах кибербезопасности от сетей и сетевых устройств

Для выявления подозрительных точек, которые могут указывать на внутренних злоумышленников, организация собирает доказательства и осуществляет мониторинг сети. Если мониторинг хост-устройств не дает результатов, то эффективность доказательств можно повысить, осуществляя мониторинг сети. Целью мониторинга сети является не предотвращение атак, а сбор информации, которая может оказаться полезной в случае инцидента, к тому же он дает гораздо больше доказательств для анализа. Инструменты сбора данных об инцидентах безопасности от сети и сетевых устройств должны обеспечивать следующие возможности:

– сбор сетевого трафика без потерь;
– извлечение потока сеанса связи из данных трассировки сети и сбор информации о потоке сеанса, такой как IP-адрес и номер порта источника, IP-адрес и номер порта назначения, IP-протокол и служебная информация, время начала и окончания сеанса, количество и размер входящих пакетов, количество и размер исходящих пакетов;
– сбор переносимых исполняемых файлов (PE), передаваемых по сети, и извлечение информации о файлах, включая имя файла, размер файла, время сбора файла, IP-адрес и номер порта источника для сеанса, содержащего переносимый исполняемый файл (файл PE), IP-адрес и номер порта назначения для сеанса, содержащего файл PE, IP-протокол;
– сбор журналов событий сетевых устройств, таких как маршрутизаторы, коммутаторы, системы мониторинга сети.

8 Требования к сохранению данных об инцидентах кибербезопасности

Чтобы проанализировать причины инцидентов кибербезопасности, необходимо сохранить собранные исходные данные и не допустить их повреждения. В частности, в случае судебных разбирательств необходимо сохранить собранные данные, чтобы целостность и законность доказательств оставались

без изменений. Для этого инструменты сохранения данных должны поддерживать следующие возможности:

– генерирование контрольных сумм и цифровых подписей;
– проверку полной сохранности собранных данных;
– генерирование меток времени (в миллисекундах) для фиксации времени сбора и сохранения данных;
– запись собранных данных на устройство однократной записи и многократного чтения (WORM);
– предоставление профиля политики хранения данных, которая должна соблюдаться надлежащим образом;
– обеспечение сохранности собранных данных в течение всего срока действия политики;
– хранение собранных данных и метаданных в формализованном виде (различные соображения по этому вопросу изложены в [b-ITU-T X.1215] и [b-ITU-T X.1541]).

9 Требования к инструментам сбора и сохранения данных для обеспечения надежности

Данные, собранные и сохраненные с помощью соответствующих инструментов, могут использоваться для расследования причин инцидентов кибербезопасности и в качестве доказательств при выявлении ответственных за инцидент.

Поэтому инструмент сбора и сохранения данных для анализа инцидентов кибербезопасности должен обеспечивать следующие возможности по гарантированию надежности, относящиеся к управлению пользователями и данными:

– инструмент должен предоставлять средства для ограничения и контроля доступа пользователей к самому инструменту и к хранимым данным;
– инструмент не должен допускать попыток перезаписи, изменения или удаления хранящихся данных без надлежащей авторизации;
– инструмент должен обеспечивать функции управления безопасностью, с тем чтобы авторизованные администраторы могли конфигурировать функции безопасности, политику безопасности и важные данные и управлять ими;
– при передаче собранных данных между физически изолированными устройствами данные должны шифроваться для обеспечения их конфиденциальности и целостности;
– во всех средствах передачи данных, связанных с инструментом, следует использовать защищенный шифрованный протокол связи;
– инструмент должен обеспечивать функцию резервного копирования сохраненных данных; и
– инструмент должен обеспечивать возможность ведения журналов событий, отчетов об ошибках и аудита;
– инструмент должен обеспечивать возможности обработки метаданных и формализованного контента и их совместного использования в соответствии с действующей политикой (как указано в [b-ITU-T X.1550] и [b-ITU-T X.1582]).

Библиография

[b-ITU-T E.409] Рекомендация МСЭ-Т E.409 (2004 г.), *Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи*.

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996), *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-ITU-T X.1215] Рекомендация МСЭ-Т X.1215 (2019 г.), *Сценарии использования структурированного представления информации об угрозах*.

[b-ITU-T X.1541] Рекомендация МСЭ-Т X.1541 (2017 г.), *Формат обмена описаниями инцидентов как объектов*.

[b-ITU-T X.1550] Рекомендация МСЭ-Т X.1550 (2017 г.), *Модели контроля доступа для сетей обмена информацией об инцидентах*.

[b-ITU-T X.1582] Рекомендация МСЭ-Т X.1582 (2014 г.), *Протоколы транспортирования, поддерживающие обмен информацией о кибербезопасности*.

[b-ITU-R BR.1351] Recommendation ITU-R BR.1351 (1998), *Requirements for the application of digital technology to audio archiving systems for radio broadcasting*.

[b-IETF RFC 2828] IETF RFC 2828 (2000), *Internet Security Glossary*.

[b-IETF RFC 3227] IETF RFC 3227 (2002), *Guidelines for Evidence Collection and Archiving*.

[b-ISO/IEC 27035-3] ISO/IEC 27035-3, *Information technology – Security techniques – Information security incident management – Part 3: Guidelines for incident response operations*.

[b-ISO/IEC 27037] ISO/IEC 27037:2012, *Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*.

[b-ISO/IEC 27041] ISO/IEC 27041:2015, *Information technology – Security techniques – Guidance on assuring suitability and adequacy of incident investigative method*.

[b-ISO/IEC 27042] ISO/IEC 27042:2015 *Information technology – Security techniques – Guidelines for the analysis and interpretation of digital evidence*.

[b-ISO/IEC 27043] ISO/IEC 27043:2015, *Information technology – Security techniques – Incident investigation principles and processes*.

[b-Jajodia14] Jajodia, Sushil, and Kun Sun. "MTD 2014: First ACM workshop on moving target defense". Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.