Международный союз электросвязи

МСЭ-Т X.1217

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(01/2021)

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

Безопасность киберпространства – Кибербезопасность

Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи

Рекомендация МСЭ-Т X.1217

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.1389
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.1217

Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи

Резюме

Оперативная информация об угрозах с точки зрения оператора электросвязи – это совокупность систематизированной, проанализированной и уточненной информации о потенциальных и текущих атаках, которые могут угрожать организации. Эта информация может включать также данные о мотивах, намерениях, характеристиках и методах злоумышленников, наряду со сведениями об их образе или методах действия, тактике и процедурах.

В сфере сетевой и информационной безопасности возникновение крупномасштабных и неожиданных нарушений кибербезопасности обусловило неотложную потребность в оперативной информации об угрозах. Оперативная информация об угрозах может помочь организации снизить риски и повысить общий уровень безопасности. Для того чтобы обеспечить возможность обмена оперативной информацией об угрозах между различными организациями, определены унифицированные классификация, грамматика и представление оперативной информации об угрозах.

В Рекомендации X.1217 представлены руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи после обзорного анализа.

Хронологическая справка

Издание	Рекомендация	Утверждено	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1217	07.01.2021 г.	17-я	11.1002/1000/14443

Ключевые слова

Безопасность, оперативная информация об угрозах.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера 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 в целях 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

Введение

Оперативная информация об угрозах с точки зрения оператора электросвязи – это совокупность систематизированной, проанализированной и уточненной информации о потенциальных и текущих атаках, которые могут угрожать организации. Эта информация может включать также данные о мотивах, намерениях, характеристиках и методах злоумышленников, наряду со сведениями об их образе или методах действия, тактике и процедурах.

В сфере сетевой и информационной безопасности возникновение крупномасштабных и неожиданных нарушений кибербезопасности обусловило неотложную потребность в оперативной информации об угрозах. Оперативная информация об угрозах может помочь организации снизить риски и повысить общий уровень безопасности благодаря пониманию того, кто вероятнее всего осуществляет нападение, на что будут направлены атаки, чего добиваются злоумышленники, зачем им это нужно и как они планируют это делать.

Язык и формат сериализации, используемые для обмена оперативной информацией о киберугрозах, определены в [OASIS STIXv2]. Протокол, используемый для обмена оперативной информацией о киберугрозах поверх HTTPS, определен в [OASIS TAXIIv2]. В [ITU-T X.1215] описан возможный порядок использования языка структурированного представления информации об угрозах (STIX) для поддержки оперативной информации и обмена информацией о киберугрозах.

Для того чтобы обеспечить возможность обмена оперативной информацией об угрозах между различными организациями, определены унифицированные классификация, грамматика и представление оперативной информации об угрозах. Следующая проблема, которую необходимо учитывать, – это способ использования оперативной информации об угрозах для решения задач обеспечения безопасности в сети.

Язык команд управления и контроля (C2) для управления функциями кибербезопасности определен в [OASIS OpenC2-L]. Интерфейс прикладного программирования (API) на основе HTTPS для передачи команд OpenC2 в устройства кибербезопасности определен в [OASIS OpenC2-H]. Управление брандмауэрми без регистрации состояния с использованием языка OpenC2 определено в [OASIS OpenC2-P]. В OASIS в стадии разработки находятся профили других функций кибербезопасности.

В настоящей Рекомендации после обзорного анализа представлены руководящие указания по применению оперативной информации об угрозах.

Рекомендация МСЭ-Т X.1217

Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи

1 Сфера применения

В настоящей Рекомендации после обзорного анализа представлены руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи.

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 источники могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ в данной Рекомендации не придает ему как отдельному документу статус Рекомендации.

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

[OASIS OpenC2-H] OASIS Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0. <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html

[OASIS OpenC2-L] OASIS Open Command Open Command and Control (OpenC2) Language Specification Version 1.0. <https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[OASIS OpenC2-P] OASIS Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0. <https://docs.oasis-open.org/openc2/oc2slpf/v1.0/oc2slpf-v1.0.html>

[OASIS STIXv2] OASIS STIX 2.1 specifications. <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>

[OASIS TAXIIv2] OASIS TAXII 2.1 specifications. <https://docs.oasis-open.org/cti/taxii/v2.1/cs01/taxii-v2.1-cs01.html>

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 бот-сеть (botnet) [b-ITU-T X.1231]: Дистанционно управляемые вредоносные программные роботы (боты), которые автономно или автоматически запускаются на зараженных компьютерах вместе с командно-управляющим сервером, принадлежащим владельцам ботов.

3.1.2 мошенничество (fraud) [b-ITU-T Y.140.1]: Акт получения материальной выгоды путем искажения фактов или несанкционированных действий.

3.1.3 вредоносное программное обеспечение (malware) [b-ITU-T X.1211]: Вредоносное программное обеспечение, созданное специально для нанесения ущерба или разрушения системы путем осуществления атак, направленных на нарушение конфиденциальности, целостности и/или доступности.

3.1.4 фишинг (phishing) [b-ITU-T X.1244]: Попытка преступным или мошенническим путем завладеть важной информацией, например именем пользователя, паролем и данными финансового счета путем маскировки под заслуживающий доверия объект в электронной связи.

3.1.5 уязвимость (vulnerability) [b-ITU-T X.1524]: Любое слабое место в программном обеспечении, которое может быть использовано для нарушения системы или содержащейся в ней информации.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 очистка данных (data cleaning): Процесс удаления нерелевантных данных и дубликатов данных в исходном наборе данных, сглаживания шума и обработки недостающих значений и выбросов.

3.2.2 отсечение данных (data clipping): Процесс удаления бесполезных или аномальных данных.

3.2.3 дедупликация данных (data deduplication): Процесс удаления повторяющихся данных в исходном наборе данных.

3.2.4 десенсибилизация данных (data desensitization): Процесс сокрытия конфиденциальных данных.

3.2.5 фильтрация данных (data filtering): Процесс удаления нерелевантных данных и проведения фильтрации посторонних данных в исходном наборе данных.

3.2.6 отображение данных (data mapping): Процесс преобразования элементов данных из исходной системы данных в целевую.

3.2.7 объединение данных (data merging): Процесс объединения аналогичных записей данных в единую запись.

3.2.8 интеллектуальный анализ данных (data mining): Вычислительный процесс обнаружения закономерностей в больших наборах данных с использованием методов искусственного интеллекта, машинного обучения, статистики и систем баз данных.

3.2.9 подавление шума в данных (data noise reduction): Процесс сглаживания шума в данных.

3.2.10 подготовка выборки данных (data sampling): Статистический метод, используемый для обработки недостающих значений и выбросов.

3.2.11 сегментация данных (data segmentation): Процесс сегментации данных с других уровней.

3.2.12 сортировка данных (data sorting): Процесс сортировки данных в определенном порядке или по категориям.

3.2.13 преобразование данных (data transforming): Процесс преобразования данных в определенный формат и масштабирования данных до заданного диапазона.

3.2.14 сбор данных об инцидентах (incidents collecting): Процесс сбора данных об инцидентах, связанных с нарушением безопасности.

3.2.15 ситуационная осведомленность (situation awareness): Процесс представления общей ситуации и прогнозирования возможных угроз и атак.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Programming Interface	Интерфейс прикладного программирования
CVE	Common Vulnerabilities and Exposures	Общеизвестные уязвимости и незащищенности
C&C	Command and Control	Управление и контроль
DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
DNS	Domain Name System	Система доменных имен
FW	Firewall	Брандмауэр
GW	Gateway	Шлюз
HTTPS	Hypertext Transfer Protocol Secure	Протокол защищенной передачи гипертекста
ID	Identity	Идентификатор
IDS	Intrusion Detection System	Система обнаружения вторжений

IP	Internet Protocol	Протокол Интернет
MD5	Message Digest Algorithm 5	Алгоритм хэширования MD5
IPS	Intrusion Prevention System	Система предотвращения вторжений
O&M	Operations and Maintenance	Эксплуатация и техническое обслуживание
SDN	Software Defined Network	Сеть с программируемыми параметрами
SIEM	Security Information and Event Management	Информация о безопасности и управление событиями
SoC	Security Operation Centre	Оперативный центр по обеспечению безопасности
STIX	Structured Threat Information expression	Структурированное представление информации об угрозах
TAXII	Trusted Automated exchange of Intelligence Information	Надежный автоматический обмен информацией об индикаторах
URL	Uniform Resource Locator	Унифицированный указатель ресурса
WAF	Web Application Firewall	Брандмауэр веб-приложения

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 настоящей Рекомендации;

ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

ключевое слово "**запрещается**" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и что функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Общие сведения об оперативной информации об угрозах

Оперативная информация об угрозах с точки зрения оператора электросвязи – это совокупность систематизированной, проанализированной и уточненной информации о потенциальных и текущих атаках, которые могут угрожать организации. Эта информация может включать также данные о мотивах, намерениях, характеристиках и методах злоумышленников, наряду со сведениями об их образе или методах действия, тактике и процедурах.

При эксплуатации сетей электросвязи оперативная информация об угрозах – это знания, используемые для предотвращения или смягчения последствий кибератак, в том числе о мотивах, намерениях, характеристиках, методах, действиях, приемах, тактике и процедурах злоумышленников. Она не связана с информацией, позволяющей установить личность.

В сфере сетевой и информационной безопасности возникновение крупномасштабных и неожиданных нарушений кибербезопасности обусловило неотложную потребность в оперативной информации об угрозах. Оперативная информация об угрозах может помочь организации снизить риски и повысить общий уровень безопасности благодаря пониманию того, кто вероятнее всего осуществляет нападение, на что будут направлены атаки, чего добиваются злоумышленники, зачем им это нужно и как они планируют это делать.

Язык и формат сериализации, используемые для обмена оперативной информацией о киберугрозах, определены в [OASIS STIXv2]. Протокол, используемый для обмена оперативной информацией о киберугрозах поверх HTTPS, определен в [OASIS TAXIIv2]. В [ITU-T X.1215] описан возможный порядок использования языка структурированного представления информации об угрозах (STIX) для поддержки оперативной информации и обмена информацией о киберугрозах.

Для того чтобы обеспечить возможность обмена оперативной информацией об угрозах между различными организациями, определены унифицированные классификация, грамматика и представление оперативной информации об угрозах. Следующая проблема, которую необходимо учитывать, – это способ использования оперативной информации об угрозах для решения задач обеспечения безопасности в сети.

Язык команд управления и контроля (C2) для управления функциями кибербезопасности определен в [OASIS OpenC2-L]. API на основе HTTPS для передачи команд OpenC2 в устройства кибербезопасности определен в [OASIS OpenC2-H]. Управление брандмауэрами без регистрации состояния с использованием языка OpenC2 определено в [OASIS OpenC2-P]. В OASIS в стадии разработки находятся профили других функций кибербезопасности.

7 Обзор применения оперативной информации об угрозах при эксплуатации сетей электросвязи

На рисунке 7-1 показано, как оперативная информация об угрозах применяется при эксплуатации сети электросвязи.

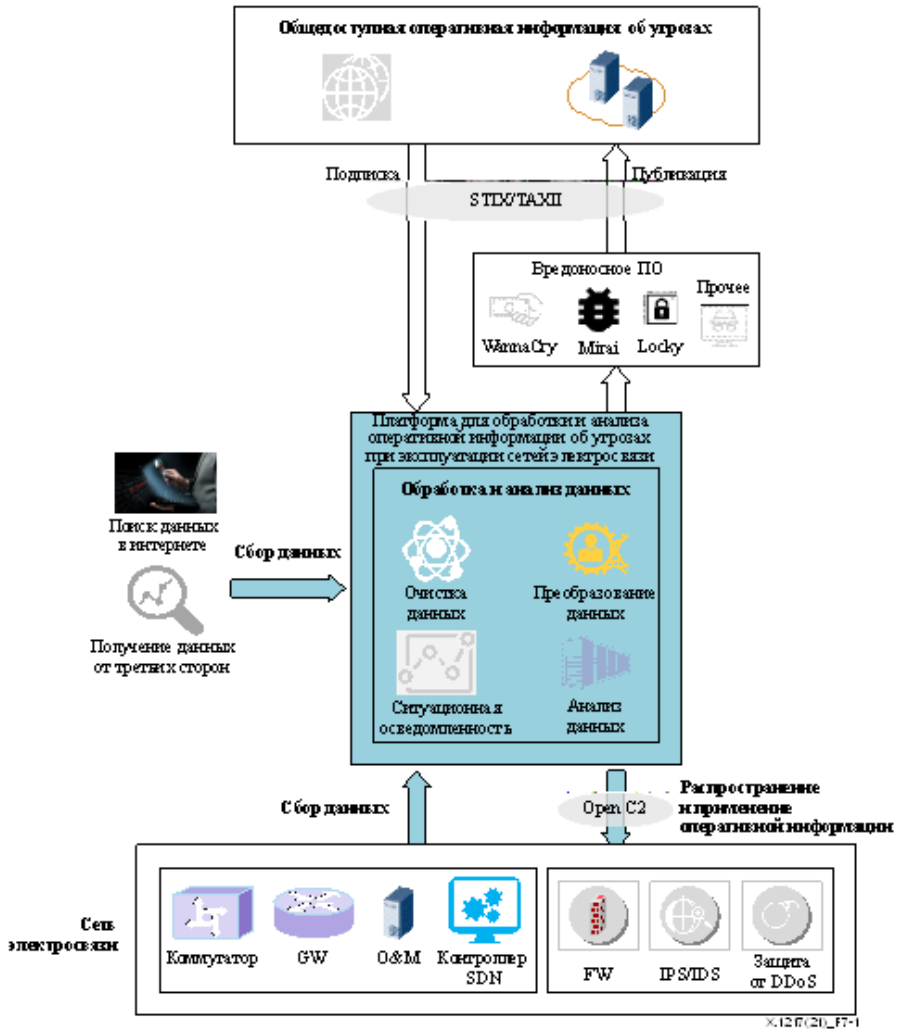

Рисунок 7-1 – Обзор применения оперативной информации об угрозах при эксплуатации сетей электросвязи

Как показано на рисунке 7-1, применение оперативной информации об угрозах при эксплуатации сетей электросвязи включает три основных процесса: сбор данных, обработку и анализ данных, а также распространение и применение оперативной информации об угрозах.

7.1 Сбор данных

Существует два типа источников данных, из которых поступает оперативная информация об угрозах:

- данные от внутренних сетевых элементов и устройств безопасности;
- данные из внешних источников.

Данные от внутренних сетевых элементов и устройств безопасности в основном включают регистрационные журналы, оповещения и политику безопасности, например журналы регистрации инцидентов, журналы системы доменных имен (DNS), журналы регистрации брандмауэров и т. д.

Данные также могут быть получены из ряда конкретных внешних источников, например, путем поиска в интернете, получения данных от третьих сторон посредством STIX/TAXII и т. д. К совместно используемым данным в основном относятся IP-адреса, доменные имена, URL-адреса, сведения об инцидентах, уязвимостях и т. д.

Перед сбором данных необходимо выполнить их десенсибилизацию.

7.2 Обработка и анализ данных

Процесс обработки и анализа данных состоит из четырех функциональных компонентов: очистка данных, преобразование данных, анализ данных и ситуационная осведомленность.

На рисунке 7-2 показаны функциональные компоненты процесса обработки и анализа данных.

Рисунок 7-2 − Функциональные компоненты процесса обработки и анализа данных

- В процессе очистки данных производится удаление нерелевантных данных и дубликатов данных в исходном наборе данных, сглаживание шума и обработка недостающих значений и выбросов.
- В процессе преобразования данных осуществляются интеграция и нормализация данных.
  - Интеграция данных заключается в приведении данных из нескольких источников к определенному формату.
  - В процессе нормализации данных осуществляется устранение влияния единиц измерения и диапазонов значений между показателями, а также масштабирование данных до указанного диапазона значений, включая преобразование функций, составление атрибутов и т. д.
- При анализе данных используются различные алгоритмы анализа данных, извлечения ключевых слов, правил очистки и корреляционного анализа для получения оперативной информации об угрозах и анализа соответствующих мер противодействия.
- Ситуационная осведомленность включает визуализацию, а также прогнозирование и предупреждение.
  - Визуализация – это визуальное отображение общей ситуации с помощью анализируемых данных, такое как классификация, сортировка и т. д.

- Прогнозирование и предупреждение – это предсказание диапазона возможных угроз, путей атаки, методов атаки и т. д. на основе анализа данных и общей ситуации, а также рассылка ранних предупреждений для выработки стратегий защиты от возможных атак.

7.3 Распространение и применение оперативной информации об угрозах

Распространение и применение оперативной информации об угрозах имеют два аспекта:

- исходя из оперативной информации об угрозах, администраторы эксплуатации и технического обслуживания могут осуществлять политику безопасности в отношении сетевых элементов и устройств безопасности;
- оперативная информация об угрозах может быть передана третьим сторонам.

К оперативной информации об угрозах, распространяемой и применяемой при эксплуатации сетей электросвязи, относится оперативная информация об угрозах, прогнозная информация и предупреждения, меры обеспечения безопасности сети и т. д.

К объектам распространения и применения оперативной информации при эксплуатации сетей электросвязи относятся сетевые элементы и устройства безопасности, такие как система обнаружения вторжений (IDS), система предотвращения вторжений (IPS), брандмауэры и устройства защиты от DDoS. Для управления устройствами безопасности и их контроля рекомендуется использовать спецификации OASIS OpenC2.

Целью распространения и применения оперативной информации при эксплуатации сети электросвязи является предотвращение инцидентов, связанных с нарушением безопасности, и смягчение их последствий, а также обеспечение оперативного и эффективного реагирования на каждый инцидент безопасности в сети электросвязи.

8 Руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи

В разделе 7 описаны три основных процесса: сбор данных, обработка и анализ данных, а также распространение и применение оперативной информации об угрозах при эксплуатации сетей электросвязи. Соответственно, в подразделах 8.1–8.3 содержатся руководящие указания по применению оперативной информации об угрозах при эксплуатации сетей электросвязи.

8.1 Сбор данных

Сбор данных является предварительным условием применения оперативной информации об угрозах, и его цель состоит в том, чтобы собрать всю информацию и данные, относящиеся к оперативной информации об угрозах. Рекомендуется, чтобы данные включали в себя данные, поступающие от внутренних элементов сети и устройств безопасности, такие как регистрационные журналы, оповещения и правила безопасности. Также рекомендуется, чтобы в эти данные входили данные из внешних источников, полученные, например, путем поиска в интернете, от третьих сторон и т. д. К совместно используемым данным в основном относятся IP-адреса, доменные имена, URL-адреса, сведения об инцидентах, уязвимостях и т. д.

Для сбора таких данных, как журналы DNS, журналы регистрации брандмауэров и т. д., рекомендуется реализовать активный сбор данных. Для сбора данных об инцидентах, связанных с нарушением безопасности, рекомендуется использовать процесс сбора сведений об инцидентах. Для сбора критически важной оперативной информации, такой как IP-адреса, доменные имена, URL-адреса, сведения об инцидентах и уязвимостях и т. д., рекомендуется использовать процесс сбора оперативной информации.

Если данные собираются от внутренних элементов сети и устройств безопасности, то процесс сбора данных может быть реализован по-разному в зависимости от типов информации (например, сведения об инцидентах или активности бот-сетей).

Сведения об инцидентах можно собирать от устройств IDS, устройств IPS, брандмауэров веб-приложений (WAF), устройств защиты от DDoS, платформы информации о безопасности и управления событиями (SIEM) и платформы оперативного центра по обеспечению безопасности (SoC). Рекомендуется, чтобы собранные сведения об инцидентах включали имя, описание, категорию и ресурсы, затронутые инцидентом. Рекомендуется указать время, когда произошел инцидент. Сведения об активности бот-сетей можно собирать от устройств DNS, IDS, WAF, устройств защиты от DDoS и т. д.

Рекомендуется, чтобы собранные сведения об активности бот-сетей включали имя, описание, категорию и ресурсы, затронутые активностью бот-сети. Рекомендуется указать время активности бот-сети.

Сбор данных из интернета может осуществляться по-разному в зависимости от их типа (например, информация об уязвимостях, вредоносные домены, вредоносные URL-адреса, вредоносные IP-адреса, информация об инцидентах и т. д.).

Информацию об уязвимостях можно получать с веб-сайтов, специализирующихся на уязвимостях, таких как веб-сайты общеизвестных уязвимостей и незащищенностей (CVE). Рекомендуется, чтобы собранная информация об уязвимости включала идентификатор, имя, описание, тип, уязвимые версии, затронутых поставщиков, уязвимые программные продукты и т. д.

Информацию о вредоносных доменах и URL-адресах можно классифицировать по типам угроз: командные (C&C), бот-сети, вредоносное ПО, троянский код, фишинг, мошенничество и т. д. Информацию о вредоносных доменах и URL-адресах можно получить с веб-сайтов, из отчетов поставщиков, отчетов третьих сторон о состоянии системы защиты и т. д. Рекомендуется, чтобы собранная информация о вредоносных доменах и URL-адресах включала сервер доменных имен, тип DNS, тип угрозы, уровень доверия и т. д.

Информацию о вредоносных IP-адресах можно получить с различных веб-сайтов, а также от некоторых поставщиков, компаний, специализирующихся на обеспечении безопасности, и т. д. Вредоносные IP-адреса можно классифицировать по типу угроз: DDoS, эксплойты, источники спама, веб-атаки, бот-сети, вредоносное ПО, C&C и т. д. Рекомендуется, чтобы собранная информация о вредоносных IP-адресах включала IP-адрес, тип угрозы, уровень доверия и т. д.

Информацию об инцидентах можно получить из новостей по безопасности или отчетов поставщиков. Рекомендуется, чтобы собранные сведения об инцидентах включали имя, описание, категорию, а также ресурсы, затронутые инцидентом.

К данным, полученным от третьих сторон, в основном относятся IP-адреса, доменные имена, URL-адреса, сведения об инцидентах, уязвимостях и т. д. Информация каждого типа аналогична указанной выше.

Когда данные собираются от внутренних элементов сети и устройств безопасности, сбор данных рекомендуется осуществлять с помощью автоматизированных инструментов или сценариев. Когда данные собираются из внешних источников, сбор данных рекомендуется осуществлять с использованием сценариев или механизма обмена данными и их совместного использования. Рекомендуется, чтобы последующая обработка собранных данных осуществлялась в стандартном формате, определенном в [OASIS STIXv2] и [OASIS TAXIIv2]. В отношении оперативной информации об угрозах, предназначенной для совместного использования, рекомендуется, чтобы сбор данных осуществлялся в стандартном формате, определенном в [OASIS STIXv2] и [OASIS TAXIIv2].

Перед сбором данных рекомендуется выполнять десенсибилизацию данных, поскольку десенсибилизация данных – это процесс сокрытия исходных конфиденциальных данных с помощью символов или данных в целях защиты конфиденциальных данных.

8.2 Обработка и анализ данных

8.2.1 Очистка данных

Очистка данных – одна из основных ступеней применения оперативной информации об угрозах, и ее цель состоит в том, чтобы очистить собранные данные, сделав их единообразными и пригодными для использования, а также подготовить их к этапу преобразования и анализа данных.

- Рекомендуется реализовать фильтрацию данных, подавление шума и дедупликацию данных.
- Рекомендуется реализовать фильтрацию данных, удаление нерелевантных данных и фильтрацию посторонних данных в исходном наборе данных.
- Рекомендуется реализовать подавление шума и дедупликацию данных, чтобы сгладить шум и удалить повторяющиеся данные в исходном наборе данных.

Поскольку собранные данные содержат данные разных типов, такие как IP-адреса, домены, URL-адреса, инциденты, уязвимости и т. д., процессы очистки данных могут различаться в зависимости от собранных данных.

Процесс дедупликации данных в основном заключается в удалении повторяющихся данных в целях экономии пространства для хранения данных. Критерии для данных разного типа различны. Что касается

IP-информации, если совпадают как IP-адреса, так и другие части записи, такие как тип угрозы, уровень доверия, то это дублированные данные и требуется дедупликация; в противном случае необходимо объединение этих данных. Что касается информации о домене, если все записи о сервере доменных имен, типе DNS, типе угрозы и уровне доверия совпадают, то это дублированные данные и требуется дедупликация; в противном случае необходимо объединение этих данных. В отношении информации об уязвимости, если совпадает идентификатор уязвимости, то это повторяющиеся данные и требуется дедупликация. Для данных некоторых других типов рекомендуется вычислить коэффициент подобия; если коэффициент подобия выше порогового значения, то требуется дедупликация.

Аналогичную информацию рекомендуется объединять в одну запись. Что касается IP-адресов, доменов, URL-адресов и информации об инцидентах, если IP-адрес, сервер доменных имен, URL-адрес и описание инцидента в двух записях одинаковы, то их можно объединить в одну запись. Для некоторых других типов данных можно вычислить коэффициент подобия. Если он находится в заданных пределах, то информацию необходимо объединить.

- Рекомендуется реализовать выборку данных, объединение данных и сортировку данных для обработки недостающих значений и выбросов и сделать данные более пригодными для реализации последнего процесса.
- Рекомендуется использовать автоматизированные инструменты фильтрации и дедупликации данных.

8.2.2 Преобразование данных

Процесс преобразования данных предназначен для устранения влияния единиц измерения и диапазона значений между показателями и масштабирования данных до указанного диапазона значений, включая преобразование функций, составление атрибутов и т. д., а также для приведения прошедших очистку данных к заданному формату с получением данных, подготовленных к анализу.

Для реализации преобразования данных рекомендуется использовать процессы отображения, отсечения и сегментации данных, чтобы преобразовать их в полезные значимые данные. Рекомендуется преобразование орфографии для приведения разных написаний к единому виду. Рекомендуется стандартизация формата, чтобы данные из разных источников данных были представлены в определенном формате. Рекомендуется конвергенция данных для создания единого хранилища данных из разных источников.

Процедуры преобразования данных каждого типа – IP-адресов, доменов, URL, уязвимостей, инцидентов – аналогичны. Рекомендуется применять правила отображения данных каждого типа, которые могут различаться в зависимости от типа данных. Например, правило отображения данных об инцидентах состоит в преобразовании полей имени, описания, категории и затрагиваемых ресурсов в поля стандартного формата. Рекомендуется привести к определенному формату информацию о брандмауэрах (FW), такую как метка времени отображения, URL запроса, имя хоста, тип атаки, содержимое атаки.

Для отсечения и сегментации данных рекомендуется реализовать процесс преобразования данных с помощью автоматизированных средств. Для преобразования орфографии рекомендуется реализовать процесс преобразования данных с помощью автоматизированных средств. В целях стандартизации формата рекомендуется, чтобы процесс преобразования данных соответствовал стандартному формату, определенному в [OASIS STIXv2] и [OASIS TAXIIv2].

8.2.3 Анализ данных

Анализ данных – критически важный этап применения оперативной информации об угрозах, направленный на использование различных алгоритмов анализа преобразованных данных, извлечения ключевых слов, правил очистки, корреляционного анализа и т. д. в целях получения оперативной информации об угрозах и анализа соответствующих мер противодействия.

Для реализации анализа данных рекомендуются процессы извлечения данных и интеллектуального анализа данных в целях получения ключевой оперативной информации об угрозах для создания предупреждающих сообщений или принятия соответствующих контрмер. Рекомендуется провести анализ поведения и корреляционный анализ инцидентов, чтобы найти полезную оперативную информацию об угрозах, такую как IP-адрес, доменное имя, хэш-сумма, информация о злоумышленнике, меры реагирования и т. д. Рекомендуется составить карту знаний и выполнить поиск угроз для сбора подробной оперативной информации об угрозах и применения контрмер и ответных действий.

Например, для обнаружения бот-сети C&C можно использовать алгоритм машинного обучения по журналам DNS. Журналы регистрации событий FW рекомендуется объединять с информацией об источниках угрозы, типе и времени атаки и другой информацией для вычисления уровня угрозы. Информацию об URL и IP-адресах можно использовать для вычисления уровня репутации.

Рекомендуется, чтобы алгоритмы анализа данных выполнялись автоматически. Рекомендуется, чтобы результат анализа данных соответствовал стандартному формату, определенному в [OASIS STIXv2] и [OASIS TAXIIv2].

8.2.4 Ситуационная осведомленность

Ситуационная осведомленность заключается в использовании результатов анализа данных для прогнозирования тенденций и выработки предупреждений, а также для одновременного отображения общей ситуации.

Для достижения ситуационной осведомленности рекомендуется обеспечить ситуационную визуализацию в целях отображения общей ситуации с помощью анализируемых данных. Рекомендуется использовать прогнозирование тенденций и предупреждение для прогнозирования диапазона возможных угроз, путей атаки, методов атаки и т. д. на основе анализа данных и общей ситуации, а также для рассылки ранних предупреждений в целях обеспечения стратегии защиты от возможных атак. Метод ситуационной осведомленности основан на алгоритмах, включающих машинное обучение, линейный анализ, вероятностную статистику и искусственный интеллект.

Рекомендуется, чтобы прогнозирование тенденций и предупреждение осуществлялись автоматически. Рекомендуется, чтобы результаты прогнозирования тенденций и предупреждающих сообщений соответствовали стандартному формату, определенному в [OASIS STIXv2] и [OASIS TAXIIv2]. Рекомендуется, чтобы при визуализации и отображении ситуации отображалась общая ситуация по данным с помощью инструментов визуализации.

8.3 Распространение и применение оперативной информации

Целью распространения и применения оперативной информации является предотвращение инцидентов, связанных с нарушением безопасности, или смягчение их последствий, а также обеспечение оперативного и эффективного реагирования на каждый инцидент безопасности в сети электросвязи.

Оперативная информация, полученная на этапе обработки и анализа данных, включая информацию об угрозах, прогнозную информацию и предупреждения, контрмеры по защите сети, политику безопасности и т. д., может передаваться другим подразделениям и сообществам операторов электросвязи. Оперативная информация может распространяться в нескольких формах. Например, ее можно распространять в форме отчетов и рекомендаций или ее можно распространять в виде указателей обнаружения.

Рекомендуется получать информацию от элементов сети, устройств безопасности, центров предупреждения и т. д. Администраторы эксплуатации и технического обслуживания могут разрабатывать политику безопасности в соответствии с полученной оперативной информацией и встраивать ее в элементы сети и устройства безопасности. При необходимости администраторы также могут обновлять версии программного обеспечения и изменять конфигурацию элементов сети и устройств безопасности.

Оперативную информацию типа URL рекомендуется применять к шлюзам, так чтобы шлюз мог обновлять свою политику безопасности, отфильтровав вредоносные URL-адреса в черный список. Ее также рекомендуется применять к IDS или IPS, обновляя правила защиты с использованием соответствующих URL-адресов.

Оперативную информацию о вредоносных доменах рекомендуется применять к DNS-серверам, чтобы те могли обновлять конфигурацию, внося вредоносные домены в черный список.

Оперативную информацию о вредоносных IP-адресах рекомендуется применять к брандмауэрам, с тем чтобы брандмауэр мог обновлять свою политику безопасности, отфильтровывая вредоносные IP-адреса. Ее также можно применять к IDS или IPS, обновляя правила защиты с использованием соответствующих IP-адресов.

Оперативную информацию об уязвимостях рекомендуется применять к элементам сети, которые могут устранять уязвимости путем обновления программного или аппаратного обеспечения. Ее также можно использовать для создания подключаемых модулей обнаружения, используя их для обновления

сканера обнаружения. Оперативную информацию можно дополнительно применять в системе реагирования на чрезвычайные ситуации для выявления инцидентов и помощи в принятии мер по предотвращению атак.

Рекомендуется, чтобы оперативная информация соответствовала стандартному формату, определенному в [OASIS STIXv2] и [OASIS TAXIIv2]. Рекомендуется, чтобы для команд управления и контроля безопасности использовались спецификации OASIS OpenC2.

Библиография

[b-ITU-T X.1211] Рекомендация МСЭ-Т X.1211 (2014 г.), *Методы предотвращения атак на базе веб-сети.*

[b-ITU-T X.1231] Рекомендация МСЭ-Т X.1231 (2008 г.), *Технические методы противодействия спаму*.

[b-ITU-T X.1244] Рекомендация МСЭ-Т X.1244 (2008 г.), *Общие аспекты противодействия спаму в мультимедийных IP-приложениях.*

[b-ITU-T X.1524] Рекомендация МСЭ-Т X.1524 (2012 г.), *Перечень общеизвестных слабых мест.*

[b-ITU-T Y.140.1] Recommendation ITU-T Y.140.1 (2004), *Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services*.

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.