TLD-OPS

Безопасность и стабильность ccTLD

Хранилище контактных данных для реагирования на инциденты • Предупреждения безопасности • Глобальное сотрудничество • Семинары

TLD-OPS — это глобальное сообщество по реагированию на технические инциденты для ccTLD и средствами ccTLD. Оно объединяет специалистов, отвечающих за безопасность и стабильность работы своих ccTLD.

192 членов*

163 ccTLD ASCII
От .ad (Андорра) до .zm (Замбия)

29 IDN ccTLD
От .ভারত (Индия) до . المغرب (Марокко)

Персонал
Более 345 экспертов по безопасности и стабильности работы ccTLD

Управление
На 100% осуществляется ccTLDs посредством Постоянного комитета TLD-OPS

Дополнительное преимущество
Повышает доступность ccTLD при реагировании на инциденты, контактных данных лиц, получении и обмене важными предупреждениями безопасности и запросами

* по состоянию на 27 ноября 2017 года. Текущий список членов представлен на главной странице TLD-OPS.

Цель сообщества TLD-OPS дать возможность операторам ccTLD по всему миру совместно обнаруживать и смягчать последствия инцидентов, которые могут повлиять на безопасность и стабильность работы сервисов ccTLD и интернета в более широком смысле, например: атаки типа «отказ в обслуживании» (DDOS), заражение вредоносным ПО и фишинг-атаки. Сообщество TLD-OPS открыто для всех национальных доменов ccTLD и в настоящий момент объединяет более 340 человек, отвечающих за безопасность и стабильность работы 192 различных ccTLD. TLD-OPS расширяет ассортимент имеющихся у членов сообщества структур, процессов и средств реагирования на инциденты, но не заменяет их.

Хранилище контактных данных

Сообщество TLD-OPS полагается на стандартный лист рассылки, который служит хранилищем контактных данных для реагирования на инциденты для ccTLD. Раз в месяц его подписчики получают автоматически создаваемые сообщения электронной почты с контактными данными всех участвующих ccTLD (контактные лица, номера телефонов и адреса электронной почты). Это повышает доступность членов TLD-OPS, поскольку у всех есть контактные данные всех остальных непосредственно в папке входящих писем, что, как правило, срабатывает также в чрезвычайных ситуациях в автономном режиме.

Предупреждения безопасности

В состав сообщества TLD-OPS входит приблизительно 65% всех ccTLD в мире, поэтому члены сообщества активно используют лист рассылки для обмена предупреждениями безопасности и запросами, для сообщений о DDoS-атаках и вредоносном ПО, использующем пространство имен ccTLD. Поскольку реагирование на инциденты тесно связано с обучением, членов сообщества призывают делиться информацией о том, как они справились с определенными ситуациями, в листе рассылки либо на регулярных семинарах TLD-OPS.

Управление

Лист рассылки TLD-OPS был создан национальными доменами верхнего уровня для внутреннего использования в 2014/2015 годах [1]. Он целиком находится под управлением сообщества ccTLD через Постоянный комитет TLD-OPS, в состав которого входит оперативный персонал ccTLD из всех пяти географических регионов (Африка, Азиатско-Тихоокеанский регион, Европа, Северная Америка, Латинская Америка и Карибский бассейн), а также представители Консультативного комитета по безопасности и стабильности (SSAC), Администрации адресного пространства интернета (IANA) и отдела безопасности ICANN. Постоянный комитет курирует повседневное функционирование листа рассылки и дальнейшее развитие «экосистемы TLD-OPS». ICANN обеспечивает

ГЛАВНАЯ СТРАНИЦА TLD-OPS
http://ccnso.icann.org/resources/tld-ops-secure-communication.htm

административную поддержку посредством секретариата ccNSO. Сервер рассылки находится на «нейтральной территории» в Центре исследований и анализа работы DNS (DNS-OARC).

Стать подписчиком не составит труда!

Стать подписчиком на лист TLD-OPS чрезвычайно просто, так как это лист рассылки электронной почты. Однако данный лист доступен только тем, кто отвечает за безопасность и стабильность работы ccTLD, чья личность подтверждена соответствующим контактным лицом по административным вопросам IANA.

Чтобы подписаться на этот лист, попросите свое контактное лицо по административным вопросам IANA отправить в секретариат ccNSO электронное письмо, в котором должны быть указаны имена, адреса электронной почты и номера телефонов основного и второго контактного лица вашего ccTLD по вопросам безопасности и стабильности. Воспользуйтесь расположенным справа шаблоном подписки, который также можно скопировать с главной страницы сообщества TLD-OPS.

Важная информация: электронное письмо с запросом на оформление подписки должно быть отправлено с действующего адреса электронной почты контактного лица по административным вопросам, который зарегистрирован в базе данных IANA [2]. Если это невозможно, необходимо скопировать этот адрес электронной почты в свое письмо с запросом на оформление подписки. В противном случае мы не сможем включить вас в число подписчиков.

Личное доверие

В основе листа рассылки TLD-OPS лежит личное доверие. Это означает, что подписчики могут указывать только собственные личные контактные данные: адрес электронной почты и номер телефона. Основная причина такого подхода в том, что модель на основе личного доверия способствует повышению уровня доверия в сообществе ccTLD, например, благодаря тому, что люди начинают узнавать друг друга по именам и встречаться на семинарах TLD-OPS. Таким образом в этом листе рассылки не разрешается указывать контактные данные, привязанные к должностям, при этом допускается указывать контактные лица, у которых основным адресом электронной почты является адрес, привязанный к должности.

Модель проверки документального подтверждения, которая обычно используется в сообществе по реагированию на инциденты, не подходит TLD-OPS, поскольку сообщество ccTLD — многочисленная группа (всего 291 ccTLD), а это означает, что при использовании этой модели будет трудно добавить в число подписчиков относительно малоизвестных людей.

Правила функционирования

Обмен информацией через лист рассылки с целью получения контактных данных ccTLD для реагирования на инциденты носит конфиденциальный характер и не должен выходить за рамки сообщества TLD-OPS.

Сведения о фактических инцидентах в системе безопасности должны выделяться с использованием цветов протокола Traffic Light (TLP) [2]: красный (информация только для конечного получателя), желтый (ограниченное распространение), зеленый (распространение в масштабе сообщества) или белый (неограниченное распространение). Сообщество TLD-OPS соблюдает определения TLP, которые были даны US-CERT [3], а цветом по умолчанию является TLP-AMBER (желтый).

Подписчики на лист рассылки не должны распространять автоматически созданные сообщения. В листе рассылки TLD-OPS не используется шифрование, чтобы подписчиком мог стать любой ccTLD. ■

Шаблон подписки

Воспользуйтесь указанным ниже форматом, чтобы подписаться на лист TLD-OPS. Эта форма также представлена для копирования на главной странице сообщества TLD-OPS.

-- Начало сообщения --
От кого: контактное лицо ccTLD по административным вопросам IANA или уполномоченный представитель
Кому: секретариат ccNSO < TLD-OPS-Admin@icann.org>
Копия: **адрес контактного лица ccTLD по административным вопросам IANA**
Тема: просьба о включении в число подписчиков на лист рассылки TLD-OPS

Уважаемый секретариат ccNSO,

Прошу включить указанных ниже лиц в число подписчиков на лист рассылки TLD-OPS. Настоящим подтверждаю, что они отвечают за общую безопасность и стабильность моего ccTLD, а я являюсь контактным лицом по административным вопросам IANA моего ccTLD или действую от его имени как уполномоченный представитель.

С уважением,

контактное лицо по административным вопросам IANA <ccTLD>

== КОНТАКТНЫЕ ДАННЫЕ ДЛЯ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ==

Контактное лицо №1 (основное):
Имя: <Имя 1> <Фамилия 1>
Адрес электронной почты: <Основной адрес электронной почты 1>, <Второй адрес электронной почты 1>
Номер мобильного телефона: +<код страны> <номер>

Контактное лицо №2 (дополнительное):
Адрес электронной почты: <Основной адрес электронной почты 2>, <Второй адрес электронной почты 2>
Адрес электронной почты: <Адрес электронной почты 2>
Номер мобильного телефона: +<код страны> <номер>
<- - ->
Контактное лицо №6:
Имя: <Имя 2> <Фамилия 2>
Адрес электронной почты: <Основной адрес электронной почты 6>, <Второй адрес электронной почты 6>
Номер мобильного телефона: +<код страны> <номер>
-- Конец сообщения --

Ссылки

[1] Итоговый отчет Рабочей группы SECIR: http://ccnso.icann.org/workinggroups/secir.htm
[2] База данных корневой зоны IANA, https://www.iana.org/domains/root/db
[3] Протокол Traffic Light: http://en.wikipedia.org/wiki/Traffic_Light_Protocol
[4] Определение TLP US-CERT: https://www.us-cert.gov/tlp

Об отделе

Брошюра Постоянного комитета TLD-OPS.
Версия 2.6, 27 ноября 2017 года.