Network Working Group
Request for Comments: 3013
BCP: 46
Category: Best Current Practice

T. Killalea
neart.org

November 2000

Службы и процедуры обеспечения безопасности, рекомендуемые для провайдеров Internet

Recommended Internet Service Provider Security Services and Procedures

Статус документа

Этот документ относится к категории Обмен опытом (Internet Best Current Practic) для Сообщества Internet и служит приглашением к дальнейшей дискуссии в целях совершенствования. Документ может распространяться свободно.

Авторские права

Аннотация

Целью настоящего документа является выражение того, что инженерное сообщество, представленное IETF, ожидает от провайдеров Internet (ISP[1]) в части обеспечения безопасности.

Назначение документа состоит не в том, чтобы определить набор требований ко всем ISP, а скорее в повышении уровня информированности ISP в части ожиданий сообщества и создания темы для обсуждения ожиданий сообщества в сфере безопасности.

Оглавление

1 Введение

Целью настоящего документа является выражение того, что инженерное сообщество, представленное IETF, ожидает от провайдеров Internet (ISP) в части обеспечения безопасности. Документ адресован ISP.

Информируя ISP о надеждах и чаяниях сообщества, последнее надеется убедить ISP в том, что принятие упреждающих мер в части безопасности не только является приоритетной задачей, но и в некоторых случаях может повысить уровень спроса на предлагаемые провайдерами услуги.

При отсутствии материальных стимулов документ не сможет оказывать влияния на бизнес-практику.

[1] Internet Service Providers - поставщики услуг Internet или, попросту, провайдеры. *Прим. перев.*

В данном документе термином ISP обозначаются организации, предоставляющие услуги доступа в сеть Internet или сетевые услуги Internet, включая услуги Web-хостинга, электронной почты и “контента”, но не ограничиваясь ими. К числу ISP в данном документе не относятся организации, предлагающие перечисленные услуги для решения внутренних задач.

В этом документе содержится набор рекомендаций ISP в части обеспечения безопасности поддержки служб реагирования на атаки[1], а также информация для пользователей в части того, что они могут ожидать от “качественных” провайдеров[2]. Очевидно, что с течением времени ожидания могут меняться. Однако документ представляет “срез” сегодняшних рекомендаций группы профессионалов в сфере развития Internet и используемых в сети технологий.

1.1 Используемые в документе соглашения

Ключевые слова необходимо (MUST), недопустимо (MUST NOT), требуется (REQUIRED), нужно (SHALL), не нужно (SHALL NOT), следует (SHOULD), не следует (SHOULD NOT), рекомендуется (RECOMMENDED), возможно (MAY), необязательно (OPTIONAL) в данном документе должны интерпретироваться в соответствии с RFC 2119 [RFC2119].

2 Контакты

Наиболее значимым ожиданием от ISP для сообщества в части безопасности является доступность коммуникационных каналов для случаев, связанных с инцидентами в области безопасности.

2.1 Контактная информация

Провайдерам Internet (ISP) следует поддерживать рекомендации [RFC2142], которые определяют почтовые ящики SECURITY (переписка по вопросам сетевой безопасности), ABUSE (переписка по вопросам недопустимого публичного поведения) и NOC (переписка по вопросам сетевой инфраструктуры). В этом же документе определяются дополнительные почтовые ящики, используемые для приёма запросов или отчётов о работе отдельных служб.

ISP может использовать URL для информации, содержащей разъяснения по перечисленным выше вопросам (например, http://www.ISP-name-here.net/security/).

Кроме того, ISP должны обеспечивать корректность и полноту информации в базах данных Whois, маршрутных реестрах [RFC1786] и иных репозиториях.

2.2 Совместное использование информации

ISP следует поддерживать ясную и чёткую политику и процедуры использования информации о связанных с безопасностью инцидентах, которые затрагивают пользователей, совместно с другими провайдерами, командами реагирования на инциденты[3], службами охраны правопорядка или прессой.

ISP следует обеспечивать процедуры реагирования на связанные с безопасностью инциденты, которые переходят границы с другими ISP.

2.3 Безопасные каналы

Провайдерам Internet следует осуществлять обмен информацией по рассматриваемым в этом разделе вопросам по безопасным каналам передачи данных[4].

2.4 Уведомления об уязвимостях и отчёты об инцидентах

ISP **следует** принимать меру по своевременному уведомлению пользователей об известных уязвимостях предлагаемого сервиса. Кроме того, при обнаружении новых уязвимостей в системе и программах следует указывать какие службы подвержены риску.

При инцидентах, воздействующих на компоненты инфраструктуры ISP провайдеру следует незамедлительно уведомить своих заказчиков о следующем:

- кто координирует действия по реагированию на инцидент;
- уязвимость;
- воздействие на службы;
- что нужно делать в ответ на инцидент;
- какие данные пользователей подвержены риску;
- что нужно делать для устранения уязвимости;
- план действий по реагированию, если таковой возможен.

Многие ISP поддерживают процедуры уведомления заказчиков о выходе из строя или неполадках в службах. Разумно использовать эти же каналы для уведомления пользователей о связанных с безопасностью инцидентах. В таких случаях уведомления могут приходить не ответственному за безопасность лицу заказчика, а человеку, которому адресованы обычные уведомления. Пользователям следует обратить на это внимание и обеспечить нужную пересылку таких уведомлений.

[1] В оригинале - attack management. *Прим. перев.*
[2] В оригинале - high quality service provider. *Прим. перев.*
[3] Incident Response Team
[4] В некоторых странах на использование защищённых каналов имеются юридические ограничения.

2.5 Группы реагирования на инциденты

Группы реагирования на инциденты в сфере информационной безопасности (CSIRT[1]) отвечают координацию и проведение соответствующих действий в случаях возникновения связанных с безопасностью инцидентов в сфере их ответственности. Ожидания сообщества Internet относительно CSIRT определены в документе "Expectations for Computer Security Incident Response" [RFC2350].

Независимо от того, имеет ли ISP группу CSIRT, ему следует обеспечить своим заказчикам хорошо известный способ получения и обработки сообщений об инцидентах от своих заказчиков. Кроме того, следует чётко документировать свои возможности по реагированию на инциденты, о которых сообщают пользователи, с информацией о наличии группы CSIRT, в сферу ответственности которой входит заказчик и куда можно направлять информацию об инцидентах.

Некоторые ISP имеют свои группы CSIRT. Однако не следует полагаться на то, что атака заказчика или атака сайта со стороны заказчика данного провайдера будут автоматически попадать в поле зрения группы CSIRT данного ISP. Зачастую группы CSIRT у ISP существуют лишь как дополнительная платная услуга и такие группы отвечают лишь за тех заказчиков, которые явно заказали (и, возможно, оплатили) подобные услуги.

Важно, чтобы ISP публиковали какие ресурсы по реагированию на инциденты и обеспечению безопасности доступны их заказчикам. Такая информация позволит заказчикам понимать свои действия при возникновении инцидентов **до того**, как инцидент случится. Заказчикам следует выяснить наличие группы CSIRT у своего провайдера и при наличии такой группы выяснить спектр предлагаемых услуг и правила пользования ими. Для информирования пользователей такую информацию лучше всего представить с использованием шаблона CSIRT, показанного в Приложении D документа "Expectations for Computer Security Incident Response" [RFC2350].

3 Правила пользования услугами

Каждому ISP **следует** иметь “Правила пользования услугами” (AUP[2]).

Если ISP предоставляет услуги доступа в Internet, пользовательские контракты должны быть согласованы с AUP. Правила AUP следует просматривать всякий раз при продлении контракта и, кроме того, ISP следует заблаговременно оповещать своих заказчиков об изменении правил.

В правилах AUP должно быть чётко указано, что пользователям разрешается и запрещается применительно к различным компонентам системы или сети, включая тип трафика, допустимого в сети. Правила AUP должны быть максимально чёткими во избежание неоднозначности или ложной трактовки. Например, правила AUP могут запрещать подмену адресов (IP spoofing).

3.1 Анонсирование правил

В дополнение к передаче правил AUP своим заказчикам ISP следует опубликовать правила в доступном месте (например, на общедоступном сайте), чтобы сообщество пользователей могло знать какие действия провайдер считает допустимыми и какие действия могут быть предприняты в ответ на недопустимое поведение.

3.2 Санкции

Правил AUP должны чётко указывать санкции, применяемые к нарушителям в случаях недопустимых действий.

3.3 Защита данных

Во многих случаях юрисдикция включает законы о защите данных[3]. Там, где такие законы применимы, ISP следует рассмотреть хранимые персональные данные и, при необходимости, зарегистрироваться в соответствующей организации, а также использовать такие данные только в полном соответствии с требованиями законодательства. С учётом глобального распространения ISP может оказаться, что локальных законов такого типа не существует - в таких случаях провайдерам следует по крайней мере ознакомиться с основными идеями защиты данных, прочтя типовой документ об их защите (например, [DPR1998]).

4 Сетевая инфраструктура

ISP отвечают за поддержку сетевой инфраструктуры своей части Internet, чтобы она:

- обеспечивала относительную устойчивость к известным уязвимостям безопасности;
- не позволяла атакующим легко перехватывать данные для их использования в последующих атаках.

4.1 Поддержка регистрационных данных

ISP обычно несут ответственность за поддержку данных, хранящихся в глобальных репозиториях типа Реестра Маршрутизации Internet (IRR[4]) и базах данных APNIC, ARIN и RIPE. Обновление таких данных следует выполнять лишь с использованием строгой аутентификации. ISP следует регистрировать адресное пространство, выделяемое для заказчиков и поддерживать публично доступную информацию об этом распределении с указанием соответствующей контактной информации.

4.2 Инфраструктура маршрутизации

Способность ISP маршрутизировать трафик корректному адресату может зависеть от политики маршрутизации, заданной в реестрах маршрутизации [RFC1786]. В таких случаях (если поддерживается реестр) следует обеспечить корректность поддерживаемой информации и возможность её обновления лишь с применением строгой аутентификации. Полномочия на обновление информации также следует ограничить.

[1]Computer Security Incident Response Team
[2]Appropriate Use Policy
[3]Data Protection Legislation
[4]Internet Routing Registry

При выборе доступных маршрутов к адресату следует принимать во внимание вопросы доверия к получаемым анонсам маршрутов. В прошлом были известны случаи, когда в результате применения ложных анонсов трафик уходил в «чёрные дыры» или перехватывался.

Для партнёров BGP **следует** использовать аутентификацию [RFC2385].

4.3 Фильтрация по адресам отправителя на входе

Входной в данном случае считается информация, направленная от краевых сайтов (пользователи) в сторону Internet.

Атакующие часто используют подставные адреса в поле отправителя. Для отвлечения внимания от своего сайта атакующие достаточно часто используют адреса из блока, выделенного атакуемому сайту, или блоков, выделенных для приватного использования [RFC1918]. Кроме того подставные адреса отправителей достаточно часто применяются для организации атак, основанных на использовании доверительных отношений между хостами.

Для осложнения атак с использованием подставных адресов отправителя ISP следует принять ряд мер. На граничном маршрутизаторе для каждого из своих заказчиков следует фильтровать весь трафик, направленный от заказчика и содержащий в поле отправителя адреса, не относящиеся к выделенному заказчику блоку. Более детальное описание такой фильтрации можно найти в [RFC2827].

Достаточно редко, но все же существуют обстоятельства, делающие невозможной такую фильтрацию (например, большие агрегирующие маршрутизаторы не могут принять на себя дополнительную нагрузку по фильтрации. Кроме того, фильтрация может осложнить жизнь мобильных пользователей. Следовательно, в ряде случаев входная фильтрация по адресам отправителей может оказаться неприемлемой, хотя в остальных случаях настоятельно рекомендуется применять такую фильтрацию.

В тех редких случаях, когда невозможно организовать фильтрацию на интерфейсе между заказчиком и ISP, заказчику следует организовать такую фильтрацию в собственной сети. В общем случае такую фильтрацию следует выполнять как можно ближе к хостам реальных пользователей.

4.4 Фильтрация по адресам отправителя на выходе

Выходной в данном случае считается информация, направленная из Internet в сторону краевого сайта (пользователя).

Сегодня в сети Internet используется множество приложений, предоставляющих хостам доступ на основе адресов IP (например, r-службы Berkeley). Такие приложения подвержены атакам с использованием подставных адресов (IP spoofing), описанным в [CA-95.01.IP.spoofing]. Кроме того, существуют уязвимости, связанные с использованием адресов, которые могут представляться локальными (например, land-атаки, описанные в [CA-97.28.Teardrop_Land]).

Для снижения уровня уязвимости заказчиков к такого рода атакам провайдерам следует выполнять приведённые здесь рекомендации. На граничном шлюзе для каждого из заказчиков провайдеру следует фильтровать весь выходной трафик, который содержит в поле отправителя адреса из блока данного заказчика.

Рассмотренные в параграфе 4.3 обстоятельства неприменимости входной фильтрации не относятся к рассмотренной здесь выходной фильтрации.

4.5 Фильтрация маршрутов

Избыточные обновления маршрутов могут использоваться атакующими как базовая нагрузка для организации DoS-атак. В любом случае эти избыточные обновления могут вести к снижению производительности..

ISP следует фильтровать получаемые анонсы маршрутов (например, для исключения маршрутов в сети, выделенные для приватного использования, предотвращения случаев создания обманных маршрутов, переключения маршрутов BGP [RFC2439], а также для агрегирования).

ISP следует использовать методы, предотвращающие избыточную нагрузку на другие части сети. Такую нагрузку могут порождать наспех созданные (nailed up) маршруты, агрессивное агрегирование и подавление маршрутов - в каждом из этих случаев оказывают влияние на другие части сети при изменении внутренней маршрутизации неподобающим способом.

4.6 Направленное широковещание (Directed Broadcast)

Протокол IP поддерживает направленное широковещание, когда пакеты, передаваемые через сеть, могут быть адресованы всем хостам некой подсети. На практике такое широковещание редко имеет смысл, однако оно активно используется для организации некоторых типов атак (прежде всего, DoS-атак, в которых широковещательные пакеты используются для усиления эффекта). Следовательно, маршрутизаторы, подключённые к широковещательным средам, **недопустимо**, настраивать на поддержку передачи таких пакетов в данную среду [RFC2644].

5 Инфраструктура системы

Методы, используемые ISP для управления своей системой, имеют критически важное значение для безопасности и надёжности сети провайдера. Повреждение системы может не оказывать существенного воздействия на производительность и функциональность, но, при этом, приводить к потере данных или риску отбрасывания части трафика (атаки с участием человека - man-in-the-middle).

Принято считать, что построение безопасной системы упрощается в случае реализации различных служб (например, электронной почты, web-хостинга и т. п.) на разных устройствах (компьютерах).

5.1 Управление системой

Доступ ко всем системам, играющим критическую роль в работе ISP (электронная почта, новости, web-хостинг), следует ограничивать, допуская к ним лишь администраторов соответствующих служб. Такой доступ следует предоставлять со строгой проверкой полномочий и использованием защищённых каналов. В критически важных

системах извне должны быть доступны лишь те порты, которые прослушиваются соответствующими службами провайдера (электронная почта, FTP и т. п.).

ISP следует использовать наиболее современные их безопасных методов организации соответствующих служб (например, IMAP/POP AUTHorize Extension for Simple Challenge/Response, [RFC2195]).

5.2 Не подключайте системы к транзитным сетям

Системы не следует подключать к сегментам транзитных сетей.

5.3 Открытые трансляторы электронной почты (Open Mail Relay)

ISP следует принимать активные меры по предотвращению возможности использования их почтовой инфраструктуры так называемыми спамерами (spammer) для анонимной рассылки нежелательной электронной почты (Unsolicited Bulk E-mail или UBE) [RFC2505]. Не все предлагаемые превентивные меры можно использовать для каждого сайта, но наиболее эффективные из приемлемых для сайта способов следует использовать.

ISP также следует строго предупреждать своих пользователей о необходимости предотвращения возможностей злонамеренного применения пользовательских систем.

5.4 Приём почты от пользователей

На приёме сообщений (message submissions) следует использовать расширение SMTP AUTH, описанное в документе SMTP Service Extension for Authentication [RFC2554].

Расширение SMTP AUTH предпочтительно использовать в системах с контролем передачи посты по адресам IP, поскольку это даёт возможность пользователям отправлять почту даже при подключении через сеть другого ISP (например, с работы) и обеспечивает большую устойчивость к подменам, а также позволяет легко переходить к использованию новых механизмов аутентификации по мере их разработки.

В дополнение к сказанному, для эффективного выполнения политики безопасности настоятельно рекомендуется для приёма сообщений от пользователей применять порт MAIL SUBMIT (587), как указано в документе Message Submission [RFC2476], взамен порта SMTP (25). В этом случае порт SMTP (25) можно ограничить в использовании только локальной доставкой почты.

Причина этого заключается в обеспечении дифференциации между локальной доставкой и трансляцией (т. е., предоставлением пользователям возможности передавать электронную почту через SMTP-сервер провайдера) почтовых сообщений. Использование SMTP без аутентификации следует ограничить только локальной доставкой.

Поскольку все большее число почтовых клиентов поддерживает расширение SMTP AUTH и порт представления сообщений (явно или путём настройки порта SMTP), провайдеры могут счесть полезным одновременное использование на приёме почты от заказчиков порта MAIL SUBMIT и системы SMTP AUTH; в этом случае порт 25 служит только для приёма внешней почты.

Описанные меры (SMTP AUTH и MAIL SUBMIT) не только защищают ISP от спама через чужие трансляторы (third-party relay), но и помогают отслеживать отправку почты в случаях рассылки спама пользователями данного провайдера.

6 Литература

[CA-95.01.IP.spoofing] "IP Spoofing Attacks and Hijacked Terminal Connections", ftp://info.cert.org/pub/cert_advisories/

[CA-97.28.Teardrop_Land] "IP Denial-of-Service Attacks", ftp://info.cert.org/pub/cert_advisories/

[DPR1998] The UK "Data Protection Act 1998 (c. 29)", http://www.hmso.gov.uk/acts/acts1998/19980029.htm

[RFC1786] Bates, T., Gerich, E., Joncheray, L., Jouanigot, J., Karrenberg, D., Terpstra, M. and J. Yu, "Representation of IP Routing Policies in a Routing Registry (ripe-81++)", RFC 1786, March 1995.

[RFC1834] Gargano, J. and K. Weiss, "Whois and Network Information Lookup Service", RFC 1834, August 1995.

[RFC1835] Deutsch, P., Schoultz, R., Faltstrom, P. And C. Weider, "Architecture of the WHOIS++ service", RFC 1835, August 1995.

[RFC1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. J. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2142] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, May 1997.

[RFC2195] Klensin, J., Catoe, R. and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.

[RFC2196] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.

[RFC2350] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", BCP 21, RFC 2350, June 1998.

[RFC2385] Heffernan, A., "Protection of BGP Sessions via the TCP MD5 Signature Option", RFC 2385, August 1998.

[RFC2439] Chandra R., Govindan R. and C. Villamizar, "BGP Route Flap Damping", RFC 2439, November 1998.

[RFC2476] Gellens R. and J. Klensin, "Message Submission", RFC 2476, December 1998.

[RFC2505] Lindberg, G., "Anti-Spam Recommendations for SMTP MTAs", BCP 30, RFC 2505, February 1999.

[RFC2554] Myers, J., "SMTP Service Extension for Authentication", RFC 2554, March 1999.

[RFC2644] Senie, D., "Changing the Default for Directed Broadcasts in Routers", BCP 34, RFC 2644, August 1999.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

7 Благодарности

Автор выражает благодарность за конструктивные комментарии Nevil Brownlee, Randy Bush, Bill Cheswick, Barbara Y. Fraser, Randall Gellens, Erik Guttman, Larry J. Hughes Jr., Klaus-Peter Kossakowski, Michael A. Patton, Don Stikvoort и Bill Woodcock.

8 Вопросы безопасности

Весь документ посвящён вопросам безопасности.

9 Адрес автора

Tom Killalea

Lisi/n na Bro/n

Be/al A/tha na Muice

Co. Mhaigh Eo

IRELAND

Phone: +1 206 266-2196

EMail: tomk@neart.org

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru

10 Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.