DNSSEC Защита Интернета

Документ доступен в Интернете по адресу:
http://dnssec-deployment.icann.org/dnsseccard.pdf

ICANN
Единый мир. Единый Интернет
http://icann.org

Преимущества для компаний и потребителей

Что это такое?

DNSSEC — это протокол, который внедряется в данный момент для обеспечения защиты системы доменных имен (DNS), глобальной телефонной книги Интернета. Люди предпочитают находить интернет-серверы по их именам (например, icann.org), но незаметно для пользователя DNS сопоставляет каждое имя с числовым адресом для передачи данных на подходящее устройство.

DNSSEC — это аббревиатура от DNS Security Extensions (расширения безопасности DNS). DNSSEC повышает уровень безопасности DNS путем включения алгоритма шифрования с открытым ключом в иерархию DNS, благодаря чему создается единая открытая глобальная инфраструктура открытого ключа (PKI) для доменных имен. Это стало возможным благодаря накопленному за десять лет опыту в области разработки открытых стандартов с участием сообщества.

В чем заключаются достоинства DNSSEC?

Поиск, защищенный с использованием DNSSEC, имеет цифровую подпись, обеспечивающую защиту от несанкционированных изменений и, как следствие, от атак, которые могут привести, например, к перенаправлению конечного пользователя на фальшивые или вредоносные сайты с целью кражи пароля. Когда они проводятся в рамках атаки на инфраструктуру организации или поставщика услуг Интернета, влиянию подвержены все пользователи организации. Такая атака часто называется засорением кэша. Защита от засорения кэша является одним из основных достоинств DNSSEC.

Однако появление одного из самых главных достоинств возможно благодаря начальным попыткам использовать эту только что созданную инфраструктуру открытого ключа для защиты не только доменных имен. Благодаря использованию DNSSEC также для распространения записей (ключей) с целью защиты электронной почты, веб-сайтов, идентификационных данных, сообщений и программ компании, и потребители могут ожидать скорого появления прямого заслуживающего доверия метода связи в пределах организации или страны. Подпись корневых доменов и доменов верхнего уровня подготавливает основу для этого.

Как можно реализовать DNSSEC?

Для компаний:

Внедрите DNSSEC в корпоративную инфраструктуру DNS (включите проверку DNSSEC)

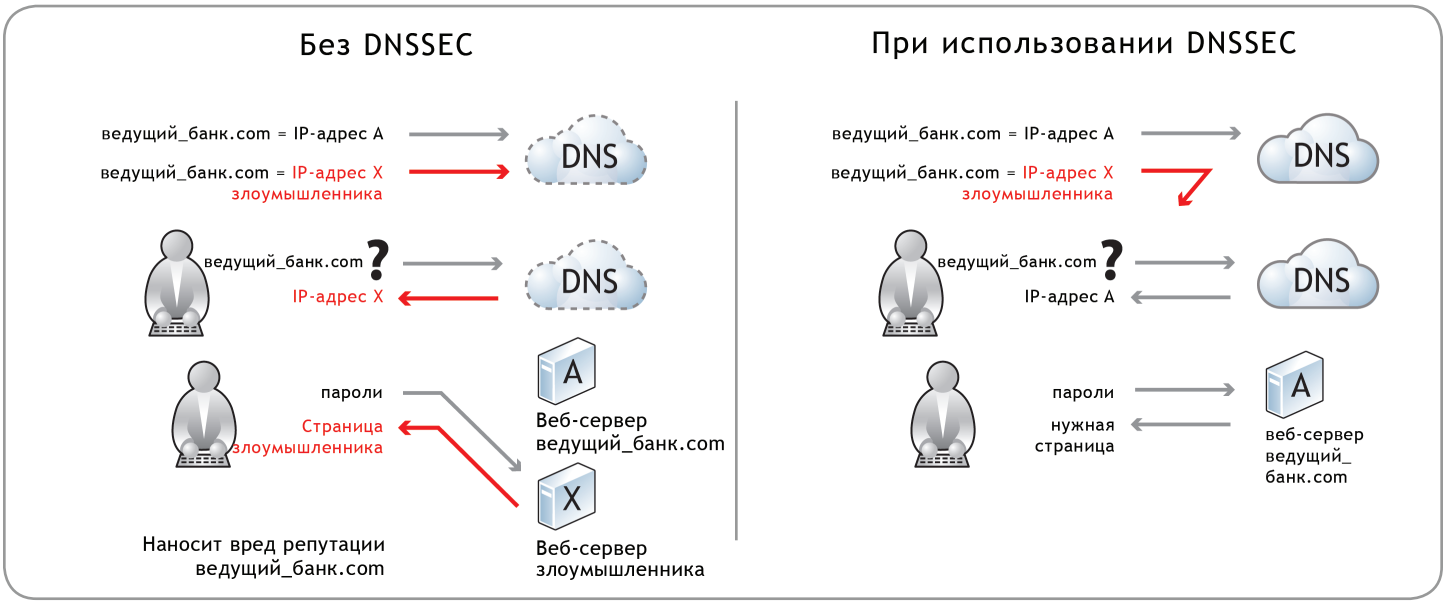
Внедрите DNSSEC в доменные имена («подпишите» корпоративные доменные имена)

Для пользователей:

Задайте вопрос относительно DNSSEC поставщику интернет-услуг (попросите включить DNSSEC на серверах DNS поставщика)

Роль ICANN

- Управление корневым ключом этой иерархии вместе с VeriSign (по договору с Министерством торговли США) и заслуживающими доверия международными представителями интернет-сообщества.
- Обработка заявок на добавление, изменение или удаление открытого ключа и других записей в регистратурах на верхнем уровне иерархии DNS (то есть .com, .se, и т. д.)
- Обучение интернет-сообщества и предоставление ему поддержки по вопросам работы с DNSSEC



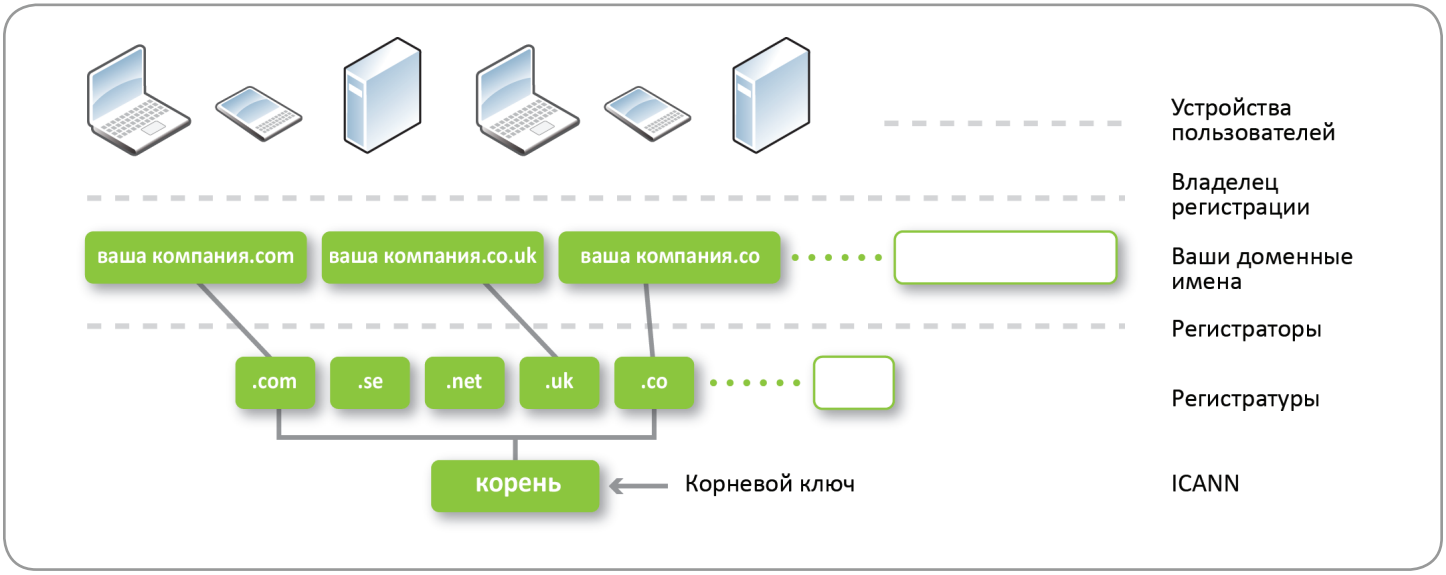
DNSSEC *Защита Интернета*

Технические консультации:

• IETF	http://www.ietf.org, http://tools.ietf.org/pdf/draft-ietf-dns op-rfc4641bis-05.pdf
• Программа внедрения DNSSEC	http://www.dnssec-deployment.org
• ISC	http://www.isc.org
• NLNETLABS	http://www.nlnetlabs.nl
• DNSSEC.NET	http://www.dnssec.net

Группы сообщества ICANN, занимающиеся DNSSEC:

- Коммерческая заинтересованная группа (CSG)
  - Группа коммерческих и деловых пользователей (BC)
  - Группы поставщиков интернет-услуг и услуг связи (ISPCP)
- Некоммерческая заинтересованная группа (NCSG)
  - Группа некоммерческих пользователей (NCUC)
- Консультативный совет по вопросам безопасности и стабильности (SSAC)



ICANN

Единый мир. Единый Интернет

http://icann.org