Groupe de travail Réseau
Request for Comments : 3013
BCP: 46
Catégorie : Bonnes pratiques actuelles

T. Killalea, neart.org

novembre 2000
Traduction Claude Brière de L'Isle

Services et procédures de sécurité recommandés aux fournisseurs de service Internet

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
L'objet de ce document est d'exprimer ce que la communauté des ingénieurs, représentée par l'IETF, attend des fournisseurs d'accès Internet (FAI) à l'égard de la sécurité.

Il n'est pas dans les intentions de ce document de définir un ensemble d'exigences qui seraient appropriées pour tous les FAI, mais plutôt de porter à la connaissance des FAI les attentes de la communauté, et de donner à cette communauté un cadre de discussion des attentes de sécurité avec les fournisseurs d'accès actuels et futurs.

Table des Matières

1. Introduction

L'objet du présent document est d'exprimer ce que la communauté des ingénieurs représentée par l'IETF attend des fournisseurs d'accès Internet (FAI) à l'égard de la sécurité. Le présent document est destiné aux FAI.

En informant les FAI de ce que cette communauté espère et attend d'eux, elle espère encourager les FAI à devenir proactifs en rendant la sécurité non seulement une priorité, mais quelque chose vers lequel ils tendent avec fierté lorsque ils vendent leurs services.

Il n'est en aucune façon dans les intentions du présent document de dicter des pratiques commerciales.

Dans le présent document on définit les FAI comme incluant des organisations dont le métier est de fournir la connexité à l'Internet ou d'autres services Internet incluant, mais sans s'y limiter l'hébergement de services de la Toile, la fourniture de contenus, et des services de messagerie électronique. On n'inclut pas dans notre définition d'un FAI les organisations qui fournissent des services pour leurs propres besoins.

Le présent document est présenté comme un ensemble de recommandations aux FAI concernant quels arrangements de sécurité et de gestion des attaques devraient être pris en charge, et comme un avis aux utilisateurs sur ce qu'ils devraient attendre d'un fournisseur de service de haute qualité. Il n'est en aucune façon normatif par lui-même. Il est vraisemblable qu'avec le temps il sera dépassé, et que d'autres attentes se feront jour. Cependant, il représente bien une photographie des recommandations d'un ensemble de professionnels du terrain à un moment donné du développement de l'Internet et de sa technologie.

1.1 Conventions utilisées dans ce document

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMETE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Communication

Les attentes les plus significatives de la communauté à l'égard des FAI en ce qui concerne la sécurité se rapportent à la disponibilité des canaux de communication pour traiter des incidents de sécurité.

2.1 Informations de contact

Les FAI DEVRAIENT adhérer à la [RFC2142], qui définit SECURITY comme la boîte aux lettres pour les questions de sécurité du réseau, ABUSE pour les questions qui se rapportent à des comportements publics inappropriés et NOC pour les questions qui se rapportent à l'infrastructure du réseau. Elle fait aussi la liste des boîtes aux lettres supplémentaires qui sont définies pour recevoir les interrogations et rapports en relation avec des services spécifiques.

Les FAI peuvent envisager d'utiliser les URL courants pour développer les détails de ce qui est exposé ci-dessus (par exemple, http://www.Nom-de-FAI-ici.net/security/).

De plus, les FAI ont pour devoir de s'assurer que leurs informations de contact, dans Whois, dans les registres d'acheminement [RFC1786] ou dans tout autre répertoire, sont complètes, précises et accessibles.

2.2 Partage d'informations

Les FAI DEVRAIENT avoir des politiques et des procédures claires sur le partage des informations sur les incidents de sécurité avec leurs clients, avec les autres FAI, avec les équipes de réponse aux incidents, avec l'application de la loi ou avec la presse et le grand public.

Les FAI devraient avoir des processus prêts à traiter les incidents de sécurité qui traversent les frontières entre eux et les autres FAI.

2.3 Canaux sécurisés

Les FAI DEVRAIENT être capables de conduire de telles communications sur un canal sécurisé. Noter cependant que dans certaines juridictions, des canaux sécurisés peuvent n'être pas permis.

2.4 Notification des vulnérabilités et rapport des incidents

Les FAI DEVRAIENT prendre l'initiative de notifier à leurs clients les vulnérabilités de la sécurité des services qu'ils fournissent. De plus, lorsque de nouvelles vulnérabilités des systèmes et des logiciels sont découvertes, ils devraient indiquer si leurs services sont menacés par ces risques.

Lorsque surviennent des incidents de sécurité qui affectent des composants de l'infrastructure du FAI, celui-ci devrait promptement rapporter à ses clients
- qui coordonne la réponse à l'incident
- la vulnérabilité
- comment le service a été affecté
- ce qui est fait pour répondre à l'incident
- si les données des clients peuvent avoir été compromises
- ce qui est fait pour éliminer la vulnérabilité
- le programme prévu pour la réponse, en supposant qu'il puisse être prévu.

De nombreux FAI ont établi des procédures pour notifier à leurs clients les pannes et les dégradations de service. Il est raisonnable que le FAI utilise ces canaux pour rapporter les incidents en rapport avec la sécurité. Dans de tels cas, le point de contact de sécurité du client peut n'être pas la personne notifiée. Le point de contact normal va plutôt recevoir le rapport. Les clients devraient savoir cela et s'assurer d'acheminer de telles notifications à la personne appropriée.

2.5 Réponse aux incidents et équipe de réponse aux incidents de sécurité informatique

Une équipe de réponse aux incidents de sécurité informatique (CSIRT, *Computer Security Incident Response Team*) est une équipe qui effectue la réponse, la coordonne, et la prend en charge, pour les incidents de sécurité qui impliquent les sites dans un domaine défini. Les attentes de la communauté de l'Internet en matière de CSIRT sont décrites dans "Attentes pour la réponse à un incident de sécurité informatique" [RFC2350].

Qu'un FAI ait ou non une CSIRT, il devrait avoir une façon bien annoncée pour recevoir et traiter les incidents rapportés par ses clients. De plus, il devrait clairement documenter ses capacités à répondre aux incidents rapportés, et devrait indiquer si il y a une CSIRT dont le domaine d'action inclurait le client et à qui les incidents pourraient être rapportés.

Certains FAI ont des CSIRT. Cependant, on devrait supposer que soit la connectivité du client du FAI, soit un site qui est attaqué par un client de ce FAI puisse automatiquement profiter lui-même des services de la CSIRT de ce FAI. Les CSIRT des FAI sont fréquemment fournis comme un service payant, dont l'équipe définit comme son domaine d'application les seules personnes qui se sont spécifiquement abonnées (et peut-être payent pour) aux services de réponse aux incidents.

Il est donc important que les FAI publient quelle réponse aux incidents et quelles ressources de sécurité sont disponibles pour les clients afin que ceux-ci puissent définir leur chaîne d'escalade de réponse aux incidents AVANT qu'un incident ne survienne.

Les clients devraient chercher à savoir si leur FAI a une CSIRT, et si c'est le cas, quelles sont la charte, les politiques et les prestations de cette équipe. Ces informations sont mieux exprimées en utilisant le gabarit de CSIRT indiqué à l'Appendice D de "Attentes pour la réponse à un incident de sécurité informatique" [RFC2350].

3. Politique d'utilisation appropriée

Chaque FAI DEVRAIT avoir une politique d'utilisation appropriée (AUP, *Appropriate Use Policy*).

Chaque fois qu'un FAI passe un contrat avec un client pour fournir la connexité à l'Internet, ce contrat devrait être gouverné par une AUP. L'AUP devrait être révisée chaque fois que le contrat est renouvelé, et de plus, le FAI devrait notifier aux clients lorsque sa politique est mise à jour.

Une AUP devrait clairement identifier ce que les clients devront faire et ne pas faire sur les divers composants d'un système ou réseau, incluant le type de trafic permis sur les réseaux. L'AUP devrait être aussi explicite que possible pour éviter les ambiguïtés ou incompréhensions. Par exemple, une AUP peut interdire l'usurpation d'identité sur IP.

3.1 Annonce de la politique

En plus de communiquer leur AUP à leurs clients, les FAI devraient publier leur politique dans un document public tel que leur site de la Toile afin que la communauté puisse savoir ce que le FAI considère approprié et puisse savoir quelle action

attendre dans le cas d'un comportement inapproprié.

3.2 Sanctions

Une AUP devrait être claire en déclarant quelles sanctions seront encourues en cas de comportement inapproprié.

3.3 Protection des données

De nombreux pays ont une législation pour la protection des données. Là où une telle législation s'applique, les FAI devraient considérer les données personnelles qu'ils détiennent et, si nécessaire, s'enregistrer comme contrôleurs de données et être prêts à n'utiliser ces données que conformément aux termes de cette législation. Étant donnée la nature mondiale de l'Internet, les FAI qui sont situés dans des pays où n'existe pas une telle législation devraient au moins se familiariser avec l'idée d'une protection des données en lisant un acte typique de protection des données (par exemple, [DPR1998]).

4. Infrastructure du réseau

Les FAI sont responsables de la gestion de l'infrastructure réseau de l'Internet d'une façon telle
- qu'il soit raisonnablement résistant aux vulnérabilités connues de la sécurité,
- qu'il ne soit pas facilement capturé par des attaquants pour l'utiliser dans des attaques ultérieures.

4.1 Maintenance des données du registre

Les FAI sont habituellement responsables de la maintenance des données qui sont mémorisées dans des répertoires globaux tels que les registres d'acheminement de l'Internet (IPP, *Internet Routing Registry*) et les bases de données APNIC, ARIN et RIPE. Les mises à jour de ces données ne devraient être possibles qu'en utilisant une authentification forte.

Les FAI devraient enregistrer publiquement l'espace d'adresse qu'ils allouent à leurs clients afin qu'il y ait plus d'informations de contact spécifiques pour l'espace délégué.

4.2 Infrastructure d'acheminement

La capacité d'un FAI à acheminer le trafic à la destination correcte peut dépendre de la politique d'acheminement telle que configurée dans les registres d'acheminement [RFC1786]. Si il en est ainsi, et si le registre le supporte, ils devraient s'assurer que les informations du registre qu'ils tiennent ne peuvent être mises à jour qu'en utilisant une authentification forte, et que l'autorité pour faire les mises à jour est restreinte de façon appropriée.

Une attention particulière devrait être apportée à déterminer à quelles annonces d'acheminement o accorde la plus grande confiance lorsque un choixde chemins est disponible pour une destination. Dans le passé des annonces erronées ont résulté en trafic enfermé dans un 'tour noir', ou pire, capturé.

L'authentification de BGP [RFC2385] DEVRAIT être utilisée avec les homologues d'acheminement.

4.3 Filtrage d'entrée sur l'adresse de source

La direction d'un tel filtrage se fait à partir du côté client de l'Internet.

Les attaquants couvrent fréquemment leurs traces en utilisant des adresses de source falsifiées. Pour détourner l'attention de leur propre site, l'adresse de source qu'ils choisissent va généralement être celle d'un innocent site distant ou bien sûr à partir des adresses qui sont allouées pour des Internets privés [RFC1918]. De plus, les adresses de source falsifiées sont fréquemment utilisées dans des attaques fondées sur l'usurpation afin d'exploiter une relation de confiance entre les hôtes.

Pour réduire l'incidence des attaques qui s'appuient sur des adresses de source falsifiées, les FAI devraient faire ce qui suit. Au routeur frontière avec chacun de leurs clients, ils devraient activement filtrer tout le trafic venant du client qui a l'adresse de source de quelqu'un d'autre que les adresses qui ont été allouées à ce client. Pour un exposé plus détaillé de ce sujet, voir la [RFC2827].

Il y a des circonstances (rares) où le filtrage d'entrée n'est actuellement pas possible, par exemple sur de grands routeurs d'agrégation qui ne peuvent pas supporter la charge supplémentaire d'appliquer les filtres de paquets. De plus, un tel filtrage peut causer des difficultés aux usagers mobiles. Donc, alors que l'utilisation de cette technique pour empêcher

l'usurpation d'identité est fortement encouragée, elle n'est pas toujours faisable.

Dans ces rares cas où le filtrage d'entrée à l'interface entre le client et le FAI n'est pas possible, le client devrait être encouragé à mettre en œuvre le filtrage d'entrée a sein de son réseau. En général, le filtrage devrait être fait aussi près que possible des hôtes réels.

4.4 Filtrage de sortie sur l'adresse de source

La direction d'un tel filtrage est de l'Internet vers le consommateur.

Il y a de nombreuses applications largement utilisées sur l'Internet d'aujourd'hui qui accordent leur confiance aux autres hôtes sur la seule base d'une adresse IP (par exemple, les commandes Berkeley 'r'). Elles sont susceptibles d'usurpation d'identité sur IP, comme décrit dans [CA-95.01]. De plus, il y a des faiblesses qui dépendent de la mauvaise utilisation d'adresses supposées locales, telles que 'land' comme décrit dans [CA-97.28].

Pour réduire l'exposition de leurs clients aux attaques qui s'appuient sur des adresses de source falsifiées, les FAI devraient faire ce qui suit. Au routeur frontière avec chacun de leurs clients, ils devraient filtrer activement tout le trafic qui va chez le client et qui a une adresse de source d'une des adresses qui ont été allouées à ce client.

Les circonstances décrites en 4.3 dans lesquelles le filtrage d'entrée n'est pas faisable s'appliquent de façon similaire au filtrage de sortie.

4.5 Filtrage de chemin

Des mises à jour d'acheminement excessives peuvent servir de levier à un attaquant comme éléments de base sur lesquels construire une attaque de déni de service. Au minimum, elles vont résulter en une dégradation des performances.

Les FAI devraient filtrer les annonces d'acheminement qu'ils voient, par exemple, en ignorant les chemins pour des adresses allouées pour des internets privés, pour éviter des chemins erronés et pour mettre en œuvre l'atténuation de fluctuation de chemin BGP [RFC2439] et la politique d'agrégation.

Les FAI devraient mettre en œuvre les techniques qui réduisent le risque de faire peser une charge excessive sur l'acheminement dans les autres parties du réseau. Cela inclut les chemins 'sans issue', l'agrégation agressive et la fluctuation de chemin, qui tous diminuent l'impact sur les autres lorsque l'acheminement interne change d'une façon qui n'est pas pertinente pour eux.

4.6 Diffusion dirigée

Le protocole IP permet la diffusion dirigée, l'envoi d'un paquet à travers le réseau pour être diffusé sur un sous réseau spécifique. Il existe très peu d'utilisations pratiques de ce dispositif, mais plusieurs attaques différentes contre la sécurité (principalement des attaques de déni de service utilisent l'effet de multiplication des paquets de la diffusion) l'utilisent. Donc, les routeurs connectés à un support de diffusion NE DOIVENT PAS être configurés d'une façon qui permette les diffusions dirigées sur ce support [RFC2644].

5. Infrastructure des systèmes

La façon dont un FAI gère son système est cruciale pour la sécurité et la fiabilité de son réseau. Une brèche dans ses systèmes peut au minimum conduire à une dégradation des performances ou fonctionnalités, mais pourrait conduire à des pertes de donnée ou au risque d'espionnage du trafic (conduisant par là à des attaques par interposition).

Il est largement accepté qu'il est plus facile de bâtir des systèmes sûrs si les différents services (comme la messagerie, les nouvelles et l'hébergement de sites) sont conservés sur des systèmes séparés.

5.1 Gestion de système

Tous les systèmes qui effectuent des fonctions critiques de FAI comme la messagerie, les nouvelles et l'hébergement de sites de la Toile, devraient être en accès restreint afin que leur accès ne soit disponible qu'aux administrateurs de ces services. L'accès ne devrait être accordé qu'à la suite d'une authentification forte, et devrait se faire sur une liaison chiffrée. Seuls les accès sur lesquels ces services écoutent devraient être accessibles de l'extérieur des réseaux système du FAI.

Les FAI devraient rester à jour des méthodes les plus sûres pour fournir les services lorsque elles deviennent disponibles (par exemple, Extension IMAP/POP AUTHorize pour mise au défi/réponse simple, [RFC2195]).

5.2 Pas de systèmes sur les réseaux de transit

Les systèmes ne devraient pas être rattachés à des segments de réseau de transit.

5.3 Relais de messagerie ouvert

Les FAI devraient prendre des mesures actives pour empêcher que leur infrastructure de messagerie soit utilisée par des 'pourriels' pour injecter de la messagerie en vrac non sollicitée (UBE, *Unsolicited Bulk E-mail*) tout en cachant l'identité de l'envoyeur [RFC2505]. Bien que toutes les mesures préventives ne soient pas appropriées pour tous les sites, les méthodes les plus efficaces appropriées à un site devraient être utilisées.

Les FAI devraient aussi encourager fortement leurs clients à prendre les mesures nécessaires pour empêcher cette activité sur leurs propres systèmes.

5.4 Soumission de message

La soumission de message devrait être authentifiée en utilisant l'extension de service AUTH SMTP comme décrit dans "Extension de service SMTP pour l'authentification" [RFC2554].

SMTP AUTH est préféré aux restrictions de soumission IP fondées sur l'adresse car elle donne aux clients du FAI la souplesse d'être capable de soumettre des messages même lorsque ils ne sont pas connectés à travers le réseau du FAI (par exemple, pendant le travail) ; il est plus résistant à l'usurpation d'identité, et peut être mis à niveau lorsque de nouveaux mécanismes d'authentification deviennent disponibles.

De plus, pour faciliter la mise en application de la politique de sécurité, il est fortement recommandé que les messages soient soumis en utilisant l'accès MAIL SUBMIT (587) comme exposé dans "Soumission de message" [RFC2476], plutôt que par l'accès SMTP (25). De cette façon, l'accès SMTP (25) peut être restreint à la seule livraison locale.

La raison en est que cela donne la capacité de différencier entre la livraison locale entrante et le relais (c'est-à-dire que cela permet à l'usager d'envoyer la messagerie via le service SMTP du FAI à des receveurs arbitraires sur l'Internet). Le SMTP non authentifié ne devrait être permis que pour la livraison locale.

Comme de plus en plus de clients de messagerie prennent en charge à la fois SMTP AUTH et l'accès de soumission de message (soit explicitement, soit par configuration de l'accès SMTP) les FAI peuvent trouver utile d'exiger que les usagers soumettent les messages en utilisant à la fois l'accès de soumission et SMTP AUTH, ne permettant que la messagerie entrante sur l'accès 25.

Ces mesures (SMTP AUTH et l'accès de soumission) non seulement protègent le FAI contre le risque de servir de point d'injection de UBE via un relais tiers, mais aussi aident à établir la comptabilité pour la soumission de message au cas où un usager envoie des UBE.

6. Références

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

[CA-97.28] "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] T. Bates, E. Gerich, L. Joncheray, J-M. Jouanigot, D. Karrenberg, M. Terpstra, J. Yu, "Représentation des politiques d'acheminement IP dans un registre d'acheminement (ripe-81++)", mars 1995. *(Information)*

[RFC1834] J. Gargano, K. Weiss, "Whois et le service de recherche d'informations de réseau, Whois++", août 1995. *(Information)*

[RFC1835] P. Deutsch, R. Schoultz, P. Faltstrom, C. Weider, "Architecture du service WHOIS++", août 1995. *(Historique)*

[RFC1918] Y. Rekhter et autres, "Allocation d'adresse pour les internets privés", BCP 5, février 1996.

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2142] D. Crocker, "Noms de boîtes aux lettres pour les services, rôles et fonctions communs", mai 1997. *(P.S.)*

[RFC2195] J. Klensin et autres, "Extension IMAP/POP AUTHorize pour mise au défi/réponse simple", septembre 1997. *(P.S.)*

[RFC2196] B. Fraser, "Manuel de la sécurité des sites", septembre 1997. (FYI0008) *(Information)*

[RFC2350] N. Brownlee, E. Guttman, "Attentes pour la réponse à un incident de sécurité informatique", juin 1998. (BCP0021)

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S.* (*MàJ par la* RFC6691)*) (Remplacée par* RFC5925)

[RFC2439] C. Villamizar, R. Chandra, R. Govindan, "Élimination des oscillations de chemin dans BGP", novembre 1998. *(P.S.)*

[RFC2476] R. Gellens, J. Klensin, "Soumission de message", décembre 1998. (*Obsolète, voir* RFC4409) *(P.S.)*

[RFC2505] G. Lindberg, "Recommandations contre les pourriels dans les MTA de SMTP", février 1999. (BCP0030)

[RFC2554] J. Myers, "Extension de service SMTP pour l'authentification", mars 1999. (*Obsolète, voir* RFC4954) *(P.S.)*

[RFC2644] D. Senie, "Changer la valeur par défaut en diffusion dirigée dans les routeurs", août 1999. (BCP0034)

[RFC2827] P. Ferguson, D. Senie, "Filtrage d'entrée de réseau : Combattre les attaques de déni de service qui utilisent l'usurpation d'adresse de source IP", mai 2000. (*MàJ par* RFC3704) (BCP0038)

7. Remerciements

Je remercie de tout cœur de leurs commentaires constructifs 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 et Bill Woodcock.

8. Considérations pour la sécurité

Ce document est tout entier consacré aux questions de sécurité.

9. Adresse de l'auteur

Tom Killalea
Lisi/n na Bro/n
Be/al A/tha na MuiceCo. Mhaigh Eo
Ireland
téléphone : +1 206 266-2196
mél : tomk@neart.org

10. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d’éditeur des RFC est actuellement fourni par la Internet Society.