Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 19 décembre 2005
N° CERTA-2005-INF-005

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Bonnes pratiques concernant l'hébergement mutualisé

Gestion du document

Référence	CERTA-2005-INF-005
Titre	Bonnes pratiques concernant l'hébergement mutualisé
Date de la première version	19 décembre 2005
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Table des matières

Secrétariat général de la défense et de la sécurité nationale – ANSSI – COSSI – CERTA
51, bd de La Tour-Maubourg **Tél.**: 01 71 75 84 50 **Web**: http://www.certa.ssi.gouv.fr
75700 Paris 07 SP **Fax**: 01 71 75 84 70 **Mél** : certa-svp@certa.ssi.gouv.fr

1 L'hébergement mutualisé externalisé

Pour des raisons financières ou techniques, beaucoup d'organisations sont tentées par l'externalisation de tout ou partie de leur système d'information.

Ce document s'adresse aux RSSI qui ont à externaliser une partie de leur système d'information, dans le but de les aider à définir le cahier des charges vu sous l'angle du traitement d'incident. Ce document se bornera donc à expliciter les clauses et aborder les pratiques permettant de pouvoir, par la suite, analyser un système de façon optimale lors d'un incident affectant une ressource dont l'hébergement est mutualisé.

Il présuppose une réflexion globale sur l'analyse des enjeux relatifs à l'externalisation de l'hébergement et l'établissement de prescriptions de sécurité différentes, auxquelles le co-hébergement ajoute des vulnérabilités particulières.

1.1 Qu'est-ce que l'hébergement mutualisé ?

L'hébergement mutualisé (ou *mutualized hosting* en anglais) consiste à héberger plusieurs ressources sur une seule et même machine, la plupart du temps gérée par une société externe. Dans la majorité des cas, les ressources mutualisées de la sorte sont des «ressources communicantes» telles que des sites web, des serveurs de messagerie, ou des ressources lourdes telles que des bases de données.

Dans ce type de solution, les clients n'ont pas accès directement aux serveurs ou aux ressources mutualisées en tant qu'administrateur. La configuration est réalisée puis gérée par un hébergeur ou une société tierce.

1.2 Pourquoi cohéberger et quelles limites ?

Le choix de l'hébergement mutualisé est principalement motivé par la réduction de l'investissement nécessaire à la gestion de la ressource. En effet :

- l'achat de matériel spécifique est inutile. Les machines sont fournies par l'hébergeur, garantissant la plupart du temps des ressources minimales (bande passante, mémoire allouée, espace disque) ;
- les coûts d'exploitation et de maintenance sont divisés entre toutes les ressources mutualisées. Le coût en ressources humaines pour l'organisation s'en trouve souvent réduit (pas d'embauche spécifique, pas de gestion des ressources humaines, possibilité de rompre le contrat à tout moment, etc.).

En contre-partie, les ressources cédées à l'hébergeur (site web, solution de messagerie, bases de données, etc.) ne sont plus totalement maîtrisées. Au delà de la prise en compte d'objectifs de sécurité spécifiques exprimés par le prescripteur pour sa ressource, l'environnement général de l'application est également exposé dans la mesure où :

- le contenu et l'utilisation des autres ressources, ainsi que leur niveau de risque, ne sont pas connus ;
- les conditions physiques d'hébergement ne sont pas toujours connues ;
- les personnels ayant accès aux informations ne sont pas toujours connus ;
- le coût des activités non prévues contractuellement n'est pas maîtrisé ;
- le procédé de mise à jour est mal maîtrisé, et souvent plus dangereux qu'un processus interne ;
- etc.

Ces points s'entendent pour des ressources dont le co-hébergement est externalisé, mais peuvent aussi être vérifiés dans le cadre d'un co-hébergement de ressources appartenant à plusieurs entités de la même organisation, géré en interne de manière centralisée, sans explication suffisante des conditions d'exploitation.

2 Risques et traitements d'incidents

2.1 Risques inhérents à l'hébergement mutualisé

L'informatique ne permet pas de concevoir des systèmes exempts de vulnérabilités. De plus, le fait d'être étroitement lié à d'autres ressources, en général de façon non maîtrisée, tend à augmenter ce risque et à en ajouter de nouveaux.

En effet, les attaques ciblant une des ressources mutualisées (réseau, logiciel, matériel) pourront avoir un impact sur l'ensemble des ressources co-hébergées. De plus, si une opération de maintenance sur une des ressources

provoque des effets de bord (indisponibilité, incompatibilité, etc.), l'ensemble des ressources sera touché, ce qui peut, à terme, inciter l'hébergeur à ne plus procéder aux mises à jour.

Un bref aperçu, non exhaustif, des risques liés au co-hébergement et de leurs répercussions suivant trois critères (disponibilité, intégrité, confidentialité) est le suivant :

Perte de disponibilité :

- une attaque par déni de service provoque l'indisponibilité du serveur hébergeant la cible de l'attaque. Si plusieurs ressources sont hébergées par le même serveur, les ressources qui n'étaient pas prises pour cible, de même que les ressources présentes sur le chemin critique (pare-feu, routeurs, etc.) sont tout de même indirectement victimes de l'attaque ;
- les ressources reposent sur un matériel qui n'est pas contrôlé par le propriétaire de la ressource, mais par l'hébergeur. Il se peut qu'un problème matériel non contrôlé ait une répercussion à plus ou moins long terme sur la ressource confiée à l'hébergeur.

Perte d'intégrité :

- un grand nombre de vulnérabilités conduisent, si elles sont correctement exploitées, à l'exécution de code arbitraire. Cette exécution de code est à la source de beaucoup de compromissions : installation d'une porte dérobée, défiguration de site web, vol d'informations, rebond d'attaques, etc.

  Si une des ressources est prise pour cible d'une telle attaque, l'exécution de code peut toucher l'ensemble des ressources ;
- un changement logiciel (voulu ou non) peut avoir une répercussion indirecte sur une ressource hébergée (non compatibilité, erreurs, etc.)

Perte de confidentialité : le fait de voir les ressources partager le même environnement physique peut conduire fréquement à du croisement d'information (contenu des fichiers clients de plusieurs sites dans la même base de données, le même sous-répertoire, etc.).

On voit donc que les risques auxquels s'expose une ressource sont augmentés de façon significative par la mutualisation de celle-ci dans un environnement non-maîtrisé.

2.2 Obstacle à la réponse aux incidents de sécurité informatique

Dans le cas d'un incident, l'hébergement mutualisé introduit par nature des obstacles à la réponse.

Par exemple, le client est rarement prévenu par l'hébergeur. L'hébergeur rétablit l'apparence de la normalité, dans le respect des délais contractualisés, quand ils existent.

Ce procédé est bien entendu contraire à la marche à suivre en cas d'incident (Cf. document du CERTA numéro CERTA-2002-INF-002). En effet, cette démarche peut détruire beaucoup de traces utiles à une analyse ultérieure permettant de retrouver le moyen utilisé pour réaliser la compromission. De plus, la machine n'est pas analysée en profondeur et la partie invisible de la compromission peut être, elle, toujours présente. Ces deux éléments conduisent souvent à de nouvelles compromissions et à l'utilisation de la ressource à des fins malveillantes.

D'autre part, lorsque l'administration propriétaire de la ressource hébergée, ou un organisme tel que le CERTA, traite une compromission, le travail de cet organisme se heurte souvent à certains problèmes :

- manque de réactivité du à la difficulté de trouver un interlocuteur chez l'hébergeur;
- mauvaises conditions d'analyses dues aux impacts éventuels sur les autres ressources hébergées :
  - refus d'isoler du réseau la machine qui héberge la ressource ;
  - refus d'établir un « périmètre de sécurité » autour de la machine ;
  - refus de laisser prélever les éléments nécessaires à l'analyse dans les règles de l'art ;
- manque d'éléments :
  - refus de communiquer les journaux d'événements (voir même un extrait) du serveur et des équipements périphériques ;
  - refus de donner une vision complète sur l'architecture du système compromis.

2.3 Cas concrets rencontrés par le CERTA

2.3.1 Serveur web mutualisé

Le CERTA a traité la compromission d'un site web sensible. Après analyse, il est apparu que la vulnérabilité exploitée par l'utilisateur mal intentionné était due à une version ancienne et vulnérable d'un forum de discussion (mis en œuvre par le logiciel `PHPbb`) hébergé par un autre site web (cf. figure1).

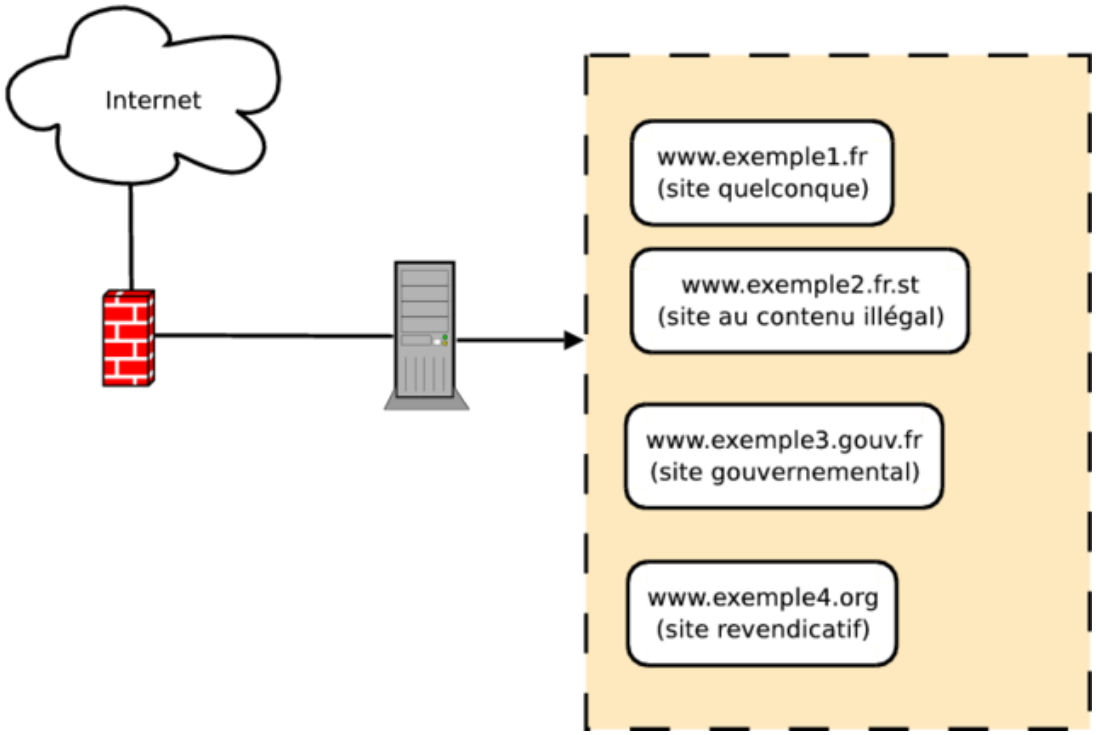

FIG. 1 – *Exemple de mutualisation de site web*

Le site d'une administration et le site affectés étaient hébergés sur le même serveur. Or, la vulnérabilité exploitée avait permis à l'attaquant d'obtenir les droits de l'administrateur sur le serveur. Ainsi, l'ensemble des sites co-hébergés sur la machine étaient impactés par l'attaque, et l'utilisateur mal intentionné disposait, entre autres, d'un contrôle total sur le site de l'administration, non vulnérable.

Dans ce cas, la partie visible de la compromission avait pris la forme d'une défiguration, mais il n'est pas exclu qu'il y ait eu vol d'informations sensibles (mots de passe, messages électroniques, bases de données, etc.), ce qui a été constaté dans des cas similaires.

2.3.2 Firewall mutualisé

Même si ce cas est original, il est tout aussi représentatif des problèmes les plus fréquents rencontrés par le CERTA.

Dans ce cas, chaque site web était hébergé sur une machine différente. En revanche, le pare-feu par lequel passait tous les flux de consultation était mutualisé entre tous les sites (cf. figure2).

Un des sites était visé par une tentative d'attaque par déni de service. L'attaque, bien que visant le site web, a provoqué un déni de service sur le pare-feu mutualisé, rendant injoignables l'ensemble des ressources, y compris celles hébergées sur des serveurs différents.

Lorsque le CERTA, à des fins d'analyse, a voulu récupérer les journaux d'événements du pare-feu (ou au moins une extraction de ces journaux), la réponse a été négative en raison des accords de confidentialité liant l'hébergeur à ses clients.

3 Recommandations

D'une façon générale, une analyse de risques devrait être systématiquement conduite, afin de mesurer les enjeux d'un co-hébergement. Une plate-forme dédiée, gérée par l'organisme lui-même, peut dans certains cas s'avérer utile au vu des besoins de sécurité nécessaires.

Si toutefois le choix de l'externalisation d'un hébergement mutualisé est retenu, il convient de bien analyser les conséquences potentielles d'attaques dans tous les cas de figure, et de contractualiser les actions permettant un traitement efficace d'un incident.

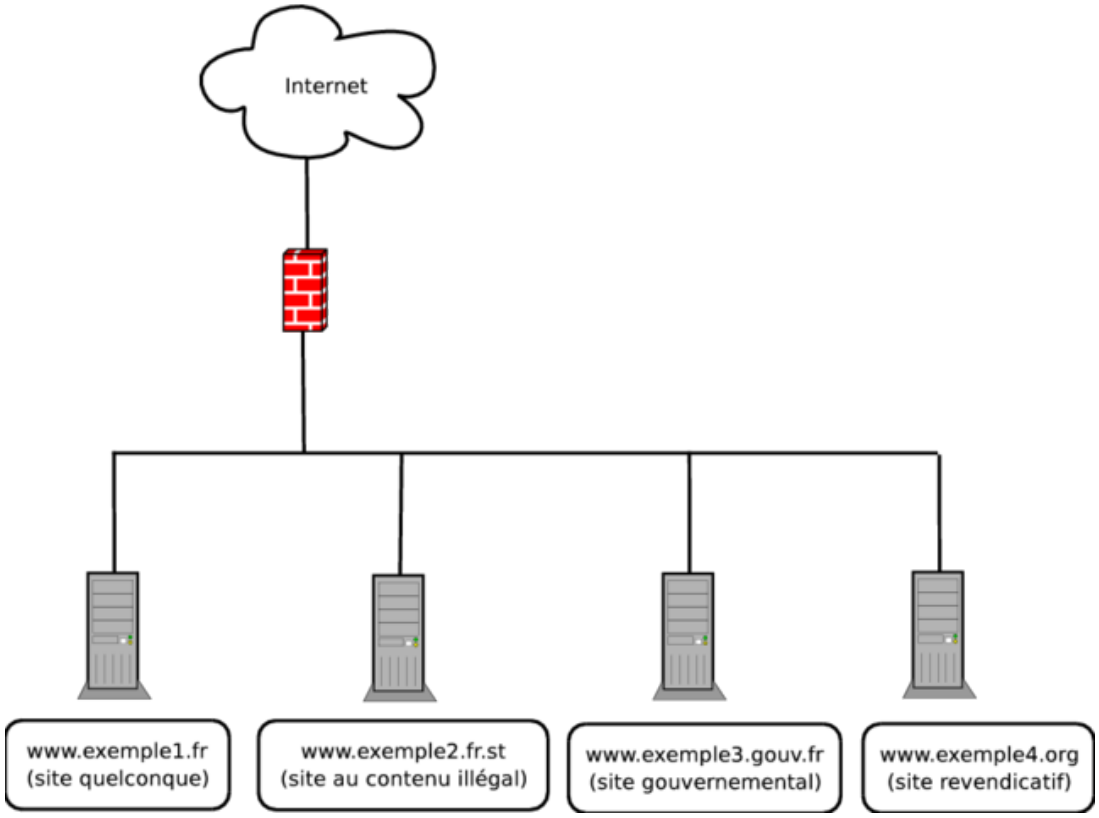

FIG. 2 – *Exemple de mutualisation de pare-feux*

En cas de recours à un co-hébergement, cinq domaines méritent ainsi de faire l'objet de prescriptions explicites, en coordination avec le service juridique :

- les journaux d'événements,
- le suivi de la ressource hébergée,
- les modalités de prévention d'une attaque,
- la réaction suite à incident,
- la réversibilité du contrat d'hébergement.

La note CERTA-2002-INF-002 du CERTA ("Les bons réflexes en cas d'intrusion sur un système d'information") peut aider à effectuer cette analyse de risque.

3.1 Journaux d'événements

Les journaux d'événements sont essentiels dans l'analyse d'un système. Des accords doivent donc être trouvés entre le client et le prestataire, afin de s'assurer de la possibilité d'accéder aux journaux d'événements, soit dans le cas d'un incident, soit à des fins de suivi de la (les) ressource(s). Il conviendra de préciser les conditions d'accès à ces journaux :

- le client doit pouvoir avoir accès aux journaux d'événements (réduits éventuellement à un extrait) à la demande du client et dans les délais contractualisés (e.g. dans la journée). L'idéal est que le client ait un moyen de suivi des événements en temps réel ;
- le client doit, de plus, être sûr que les journaux concernant ses ressources hébergées ne sont pas divulgués à d'autres organismes co-hébergés (garantie de confidentialité).
- l'hébergeur doit certifier que toutes les informations présentes sur les journaux sont exploitables au regard de l'état de l'art (pas de biais horaire ou biais horaire maîtrisé et documenté, journaux déportés ou copiés sur une autre machine, etc.)

3.2 Suivi de la ressource co-hébergée

Outre le contrôle des journaux d'événements, le fait de pouvoir disposer d'indicateurs sur l'historique de la ressource hébergée peut être appréciable. Ainsi, il est possible de dégager les principaux événements relatifs à l'utilisation de la ressource, ce qui permet d'avoir accès à des évenements ayant précédé une éventuelle crise. Les indicateurs appréciables sont (liste non exhaustive) :

- fréquence et suivi des mises à jour effectuées ;
- durée d'indisponibilité maximum et suivi de ces indisponibilités;
- fréquence des sauvegardes et tests de restauration effectués;
- indicateurs sur les ressources dont l'accès et la mise à disposition ne dégradent pas la sécurité du système d'information :
  - charge réseau pour le serveur et pour la ressource;
  - charge processeur utilisée par la ressource et pourcentage de la charge du serveur;
  - charge mémoire utilisée par la ressource et pourcentage de la charge du serveur;
  - etc.

De la même manière, il est préférable que le client connaisse au préalable l'origine et/ou la teneur des ressources co-hébergées, ce qui permettra d'étayer son analyse de risque.

Dans le meilleur des cas, il conviendra d'opter pour une solution hybride du co-hébergement. Celle-ci consiste à n'héberger sur un serveur donné qu'un ensemble de ressources, appartenant toutes à la même organisation, ou fruit d'une communauté d'intérêt. Il sera alors plus facile d'obtenir un accord écrit de la communauté sur l'accès à la machine pour analyse en cas d'incident.

3.3 Prévention d'une attaque

Une partie du contrat passé avec l'hébergeur doit prévoir le cas d'éventuelles attaques informatiques. La réactivité en cas d'incident étant extrêmement importante, il conviendra de faire figurer dans le contrat les points suivants :

- identification d'un contact technique (ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le client, joignable 24/24, 7/7, tous les jours de l'année;
- identification d'un contact décisionnel(ou plusieurs) clairement identifié chez l'hébergeur ainsi que chez le client, joignable 24/24, 7/7, tous les jours de l'année;
- garantie d'information immédiate : le client doit être tenu informé sans délais en cas d'attaque afin de déclencher le circuit de réaction adéquat ;
- définition des procédures de remontée d'incident ;
- définition claire et exhaustive avec l'hébergeur de ce que l'on entend par incident (défiguration, temps d'indisponibilité, etc.).

3.4 Réaction sur incident

En cas d'incident, le client seul doit avoir le contrôle total sur la marche à suivre. Ainsi, le contrat doit prévoir que :

- la désignation de l'organisme chargé de traiter l'incident doit être laissée à la seule appréciation du client ;
- Cet organisme doit pouvoir jouir au nom du client d'un contrôle total de l'environnement de la ressource à des fins d'analyse. Par exemple :
  - prélèvement de tout élément nécessaire à l'analyse conformément aux règles de l'art ;
  - analyse du système en fonctionnement.
- la gestion de l'incident et de la conduite des actions postérieures sont à la seule initiative du client. Ceci comprend :
  - toute action sur la machine : redémarrage, arrêt, rétablissement d'une sauvegarde, isolement physique du reste du réseau, établissement d'un périmètre de sécurité, etc. ;
  - délai d'indisponibilité de la ressource ;
  - délai d'indisponibilité du serveur et pénalités d'astreinte éventuelles;
  - contrôle sur les règles de filtrage.

3.5 Réversibilité du contrat de cohébergement

La ressource ne doit en aucun cas être bloquée par le contrat d'hébergement mutualisé.

Ainsi, une clause de réversibilité doit apparaître dans le contrat. Cette clause doit permettre au client de reprendre la gestion de sa (ses) ressource(s). Cette clause pourra en particulier être activée pour des raisons de sécurité (changement dans l'actionnariat du prestataire, de délocalisation des sites d'hébergement, etc.).

Le prestataire s'engage à apporter son assistance durant toute la période de migration.

Le prestataire s'engage à garantir la sécurité des données et des applications qui lui ont été confiées lors de leur transfert.

Le prestataire s'engage enfin à restituer et/ou à tenir à disposition tout élément correspondant à un extrait de l'ancien environnement d'hébergement (journaux d'événements déportés, sauvegardes, etc.) pendant une période à déterminer.

4 Conclusions

Au seul examen des termes financiers et organisationnels, il est vrai que l'hébergement mutualisé peut être une offre attractive.

En revanche, les avantages apparents offerts par une telle solution peuvent être mis à défaut par une plus grande exposition aux risques de compromission. Les conséquences d'un éventuel incident de sécurité informatique se voient aggravées par la dégradation technique des conditions de traitement et des délais de réaction accrus.

Il convient donc d'analyser avec l'attention nécessaire les conditions devant accompagner une décision d'hébergement mutualisé et de contractualiser un certain nombre de paramètres afin d'optimiser le contrôle de la (ou des) ressource(s) soumise(s) à hébergement en cas d'incident. En tout état de cause, une solution d'hébregement dédiée doit être privilégiée dans la mesure du possible.

5 Documentation

- Document du CERTA numéro CERTA-2002-INF-002-001 : *Les bons réflexes en cas d'intrusion sur un système d'information*
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
- Document du CERTA numéro CERTA-2004-ALE-001 : *Obstacles à la résolution d'incidents*
  http://www.certa.ssi.gouv.fr/site/CERTA-2004-ALE-001/index.html
- Numéro 54 de la revue *Sécurité informatique* du CNRS :
  http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num54.pdf

Gestion détaillée du document

15 octobre 2005 version initiale.