Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 octobre 2013
N° CERTA-2013-ACT-040

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-040

1 - Publication d'un guide de bonne configuration BGP

Les études menées par l'observatoire de la résilience de l'Internet français ayant fait ressortir le besoin de recenser les bonnes pratiques d'interconnexion BGP, un guide a été rédigé sur le sujet et vient d'être publié. Ce travail a été effectué par l'ANSSI en collaboration étroite avec plusieurs intervenants français.

Les éléments présentés dans ce guide portent sur la sécurité des interconnexions, le filtrage des annonces BGP, ainsi que sur d'autres aspects plus généralistes comme la journalisation. Pour chaque bonne pratique, des extraits de configuration pour quatre implémentations (Alcatel-Lucent, Cisco, Juniper et OpenBGPD) sont proposés.

Le CERTA recommande la mise en œuvre des mesures présentées dans ce guide sur les équipements de routage concernés.

Documentation

- Guide des bonnes pratiques BGP :
  http://www.ssi.gouv.fr/bonnes-pratiques-bgp

2 - Guide d'hygiène de la sécurité informatique

Le directeur général de l'ANSSI, M. Patrick PAILLOUX, est revenu à l'occasion de son discours d'ouverture des Assises de la Sécurité à Monaco sur l'importance du respect des règles d'hygiène informatique.

Depuis Octobre 2012, l'ANSSI publie un guide d'hygiène informatique qui, au travers de quarante recommandations, fourni aux entreprises les principes de base à appliquer pour sécuriser leurs systèmes d'information et protéger leur patrimoine.

Quotidiennement, le CERTA est amené à traiter des incidents qui auraient pu être évités si des recommandations telles que l'application des mises à jour de sécurité, la mise en oeuvre d'une véritable politique de mots de passe, le cloisonnement des réseaux et la sensibilisation des employés avaient été *a minima* respectées.

Afin de faciliter la diffusion de ce guide à l'international il sera bientôt disponible en langue anglaise.

Documentation

- Discours du directeur général de l'ANSSI aux Assises de la sécurité 2013 :
  http://www.ssi.gouv.fr/fr/anssi/evenements/discours-de-patrick-pailloux-directeur-general-de-l-anssi-lors-des-assises-de.html
- Guide d'hygiène informatique
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 - Volumes de données non maîtrisés

Le CERTA a récemment été amené à traiter un nouvel incident relatif à l'envoi non maîtrisé de données vers Internet.

Le CERTA rappelle que les flux réseaux entrants et sortants d'une entité doivent faire l'objet d'un contrôle régulier et minutieux.

En particulier, l'échange d'un volume important de données depuis le réseau local vers Internet doit éveiller l'attention des administrateurs, car ces échanges peuvent constituer ou masquer une exfiltration d'informations, voire l'exploitation d'une attaque par rebond.

En cas de détection d'un échange suspect, le CERTA recommande de vérifier les domaines et adresses IP destinataires de flux de données important, et de valider la légitimité des échanges auprès de l'émetteur.

En outre, si l'organisme externalise le stockage de ses données, les risques de perte de maîtrise du système d'information doivent être évalués. Pour s'en prémunir, l'ANSSI a publié « le guide d'externalisation des systèmes d'information ».

Documentation

- Guide d'externalisation des systèmes d'information :
  http://www.ssi.gouv.fr/IMG/pdf/2010-12-03_Guide_externalisation.pdf
- Bulletin d'actualité CERTA-2013-ACT-014 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-014

4 - Rappel des avis émis

Dans la période du 27 septembre au 03 octobre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-546 : Vulnérabilité dans EMC VPLEX
- CERTA-2013-AVI-547 : Multiples vulnérabilités dans Apple iOS
- CERTA-2013-AVI-548 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-549 : Vulnérabilité dans ProFTPD
- CERTA-2013-AVI-550 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-551 : Multiples vulnérabilités dans Xen
- CERTA-2013-AVI-552 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-553 : Vulnérabilité dans Cisco IOS XR

Gestion détaillée du document

04 octobre 2013 version initiale.