Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 novembre 2013
N° CERTA-2013-ACT-047

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-047

1 Retour d'expérience suite à une fuite d'information

Le CERTA a récemment été amené à traiter une affaire de fuite d'information concernant des identifiants de connexion à des services d'administration à distance de type réseau privé virtuel (VPN). Ces identifiants étaient disponibles dans un fichier texte déposé dans un répertoire non protégé du serveur web d'un prestataire de service. Le fichier avait également déjà été indexé et mis en cache par plusieurs moteurs de recherche.

Le CERTA tient à profiter de cet incident pour rappeler quelques principes de sécurité : il est important de mettre en place une gestion adéquate des mots de passe, de mettre en place une configuration correcte de serveur web et de vérifier les droits d'accès à un système d'information.

La génération et le stockage sécurisé des mots de passes sont une composante essentielle d'une gestion saine d'un système d'information. Les mots de passes doivent ainsi respecter les bonnes pratiques en matière de longueur et de complexité et être stockés de manière sécurisée dans un logiciel adapté (tel que KeePass par exemple).

Par ailleurs, les serveurs web mettant à disposition des données (informations, mises à jour techniques, etc.) se doivent d'être correctement configurés afin de ne pas permettre l'accès à des données sensibles. Une attention particulière doit être portée sur les données réellement mises à disposition, sur la restriction des accès à ces données (authentification, gestion des droits, etc.) et sur la journalisation de ces accès.

Plus généralement, les accès au système d'information d'une entité doivent être contrôlés, filtrés et journalisés. Le recours à des sociétés d'infogérance ne doit pas en faire perdre la maîtrise et ces accès doivent être restreints au maximum.

Documentation

- Guide de recommandations sur les mots de passe :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html
- Guide de recommandations pour la sécurisation des sites web :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html
- Guide sur la gestion de l'externalisation :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html
- Liste des produits certifiés CSPN (dont KeePass) :
  http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/

2 De la nécessité des sauvegardes

Un programme malveillant, *cryptolocker*, a récemment impacté de nombreux utilisateurs, aussi bien dans le domaine grand public que dans le domaine professionnel. Il s'agit d'un membre de la famille des rançongiciels : il

met en place un chiffrement des fichiers du poste qu'il infecte, et exige de l'utilisateur le paiement d'une rançon afin de lui rendre l'accès aux fichiers.

Ce type de menaces peut être assimilé au cas plus général de perte d'accès à des données informatiques. Cette perte d'accès peut également survenir à la suite d'une défaillance matérielle, comme celle d'un disque dur par exemple.

Une solution de sauvegarde des données (*backup*) permet de répondre à toutes ces problématiques. La mise en place d'un Plan de Continuité ou d'un Plan de Reprise d'Activité, telle que recommandée dans le guide d'hygiène informatique publié par l'ANSSI, inclut cette mesure.

Le CERTA recommande la mise en place de ces procédures indispensables ainsi qu'un test régulier de la capacité à restaurer ces achives, afin de pouvoir réagir rapidement et efficacement en cas de nécessité.

Il conviendra de faire attention, dans le cadre de la restauration de données pour faire face à un code malveillant, à utiliser une archive saine qui prédate l'infection.

Documentation

– Guide d'hygiène informatique :
http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 Déni de service par amplification CHARGEN

Le CERTA a récemment traité une attaque en déni de service (en anglais DDoS) se basant sur des services *CHARGEN*. Cette technique de DDoS, bien qu'ancienne, est encore parfois utilisée. Plusieurs entités du secteur financier ont été par exemple ciblées cette année.

CHARGEN (Character Generator Protocol) est un service conçu à l'origine pour générer du trafic sur le réseau afin de réaliser des mesures de bande passante ou de qualité de service. Il peut fonctionner avec le protocole UDP : lorsqu'un client envoie un datagramme UDP vers le port 19 d'un serveur *CHARGEN*, ce dernier renvoie un datagramme UDP au client contenant un nombre aléatoire de caractères.

Le principe du DDoS par amplification *CHARGEN* est le même que celui de l'amplification DNS et s'appuie sur le fait que le protocole UDP soit "non connecté". Un attaquant va envoyer des datagrammes UDP à des serveurs *CHARGEN* accessibles depuis l'Internet en usurpant l'adresse IP de sa victime. Cette dernière recevra alors les réponses des serveurs *CHARGEN*, contenant entre 200 et 1000 fois plus de données que les datagrammes UDP initiaux de l'attaquant.

Il est nécessaire de s'assurer qu'aucun service *CHARGEN* ne soit accessible depuis l'Internet pour éviter d'être impliqué dans une attaque contre une autre entité, et de saturer sa propre bande passante. Il est à noter qu'outre les serveurs applicatifs, les équipements réseau (routeurs, pare-feux, etc.) et plus généralement tous les équipements connectés au réseau sont à prendre en considération. On retrouve, par exemple, beaucoup d'imprimantes connectées au réseau possédant un service *CHARGEN* actif.

Tout service fournissant une réponse de taille supérieure à la requête initiale et n'étant pas basé sur un protocole connecté peut être utilisé pour réaliser des attaques en déni de service par amplification. Une bonne pratique consiste à lister tous les services disponibles sur le réseau, à désactiver ceux qui sont inutilisés et à ne les rendre accessibles depuis l'Internet que si un besoin métier le justifie, moyennant un filtrage en amont des adresses IP source autorisées à y accéder.

Un service non légitime accessible depuis l'Internet par défaut est aussi symptomatique d'un problème de sécurité plus important : la bonne gestion des flux entrants et sortants. Il est indispensable de s'assurer que seuls les flux identifiés comme nécessaires sont autorisés. L'ANSSI propose un ensemble de recommandations pour définir une politique de filtrage réseau adaptée aux contraintes métier et aux besoins de sécurité.

Le CERTA recommande aussi la lecture de la note d'information publiée le 14 janvier 2013 sur les dénis de service. Cette note donne des orientations pour se préparer à l'éventualité d'une attaque et pour en réduire les impacts.

Documentation

– Bulletin d'actualité du CERTA du 05/04/13 sur les Dénis de services par amplification DNS :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-014

– Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu : http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/recommandations-pour-la-definition-d-une-politique-de-filtrage-reseau-d-un-pare.html
– CERTA-2012-INF-001-001, "Dénis de service - Prévention et réaction" : http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html

4 Rappel des avis émis

Dans la période du 15 au 21 novembre 2013, le CERTA a émis les publications suivantes :

– CERTA-2013-AVI-639 : Vulnérabilité dans Apple iOS
– CERTA-2013-AVI-640 : Vulnérabilité dans Google Chrome
– CERTA-2013-AVI-641 : Vulnérabilité dans VMware
– CERTA-2013-AVI-642 : Multiples vulnérabilités dans les produits Mozilla
– CERTA-2013-AVI-643 : Vulnérabilité dans Opera
– CERTA-2013-AVI-644 : Vulnérabilité dans nginx
– CERTA-2013-AVI-645 : Multiples vulnérabilités dans Drupal

Gestion détaillée du document

22 novembre 2013 version initiale.