Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2013
N° CERTA-2013-ACT-021

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-021

1 Recommandation de sécurité relatives aux ordiphones

Une note technique de recommandation de sécurité relatives aux ordiphones a été publiée par l'ANSSI le 22 mai 2013.

Les ordiphones sont de plus en plus intégrés aux systèmes d'information, mais leur impact sur la sécurité des SI n'est pas toujours bien identifié. La note publiée décrit plusieurs scénarii d'attaques pouvant aboutir à des fuites d'informations. Elle propose des recommandations permettant de limiter les risques engendrés par le déploiement de ces équipements, dont :

- la mise en place de solutions de gestion de terminaux mobiles, afin de faciliter le déploiement centralisé de profils de sécurité ;
- l'emploi et le renouvellement régulier de mots de passe forts pour le verrouillage de l'appareil ;
- la restriction des possibilité d'installation d'applications tierces, la validation des applications déployées (ainsi que des autorisations demandées par ces dernières) et la mise à jour régulière de ces applications ;
- la désactivation des interfaces sans fil ou sans contact, lorsqu'elles ne sont pas utilisées, ainsi que le chiffrement des données et des communications sensibles ;
- la mise à jour régulière et automatique du système d'exploitation.

La note décrit également plusieurs scénarii d'attaques pouvant aboutir à des fuites d'informations.

Le CERTA recommande la lecture de cette note et l'application des mesures qu'elle propose.

Documentation

- Recommandations de sécurité relatives aux ordiphones :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-solutions-de-mobilite/recommandations-de-securite-relatives-aux-ordiphones.html

2 Campagne de phishing transmise par des serveurs légitimes

Le CERTA a récemment traité un incident relatif à l'envoi de mèls de phishing.

Dans cette affaire, l'attaquant a pu obtenir les identifiants de la boîte mèl professionnelle de la victime au moyen d'un courriel initial lui demandant de renseigner ses identifiants sur un formulaire Web. Cette boîte mèls professionnelle étant hébergée au sein de l'organisme et aisément accessible depuis l'Internet, l'attaquant a pu accéder illégitimement et consulter ou modifier le contenu des messages et du carnet d'adresses de la victime.

L'attaquant a également utilisé cet accès pour poursuivre sa campagne de phishing depuis la boîte mèl de la victime. Plusieurs milliers de courriels demandant de renseigner ses identifiants de connexion dans un formulaire Web malveillant ont ainsi été envoyés en usurpant le nom de la victime.

Les destinataires de ce courriel malveillant ont pu se laisser abuser par ce message dont l'adresse d'expéditeur est légitime, et dont une vérification des en-têtes du message montrera que le courrier provient effectivement des serveurs de l'organisme auquel appartient la victime.

Cette attaque aurait pu être beaucoup plus grave si l'attaquant avait envoyé des courriels piégés ciblés, par exemple aux émetteurs de messages reçus par la victime.

Pour se protéger de ce type de compromission, le CERTA recommande, en plus de la sensibilisation des utilisateurs, de mettre en place une solution d'authentification forte et de filtrage pour tous les services fournis par un organisme et accessibles depuis l'Internet.

Documentation

- Guide d'hygiène informatique, chapitre IV « Authentifier l'Utilisatgeur » :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Référentiel Général de Sécurité, Annexe B3 « Règles et recommandations concernant les mécanismes d'authentification » :
  http://www.ssi.gouv.fr/IMG/pdf/RGS_B_3.pdf

3 Mot de passe du compte administrateur local sous Windows

Dans le bulletin d'actualité CERTA-2013-ACT-017 publié le 26 avril 2013, le CERTA recommande l'utilisation d'un mot de passe administrateur local différent pour chacun des postes utilisateur du système d'information. Cette mesure a pour objectif de ne pas exposer l'intégralité du réseau d'entreprise si un compte administrateur local est compromis.

En cas de difficultés à mettre en œuvre cette mesure, le CERTA recommande d'interdire l'authentification à distance des comptes administrateurs locaux. Dans un environnement Microsoft Active Directory, cette mesure peut être appliquée en configurant les stratégies de groupe.

Les recommandations suivantes décrivent les bonnes pratiques à mettre en œuvre en termes de gestion des mots de passe dans un environnement Microsoft Active Directory.

3.1 Interdire la connexion par le réseau des comptes locaux membres du groupe Administrateurs

Lorsqu'un attaquant dispose des droits d'administrateur sur une machine Windows, il lui est possible de récupérer les empreintes LM ou NTLM des comptes utilisés sur cette machine. Avec cette empreinte, il peut alors s'authentifier à toutes autres machines sur lesquelles ce compte est valide, sans avoir besoin de « casser » le mot de passe (cette technique est dénommée *pass the hash*). Ce procédé est particulièrement problématique dans le cas du compte local Administrateur, systématiquement actif sur tout système Windows jusqu'à XP et Serveur 2003. Pour les systèmes plus récents (à partir de Vista et Serveur 2008) le compte Administrateur local est désactivé par défaut.

Afin d'empêcher l'utilisation des empreintes d'un compte Administrateur local d'une machine à une autre, il est possible d'en interdire la connexion à distance via le réseau en ajoutant le compte Administrateur à la stratégie « Refuser l'accès à cet ordinateur depuis le réseau ».

Pour conserver une capacité d'administration à distance des postes, il est possible d'utiliser un groupe d'utilisateurs du domaine (important: ce compte ne doit pas disposer de droit d'administration sur le domaine). Ce groupe appartiendra au groupe Administrateurs local de tous les postes utilisateur, mais pas des serveurs ni des

postes des administrateurs. Par ailleurs, cette action limitera les conséquences d'une récupération en mémoire de l'empreinte du mot de passe d'un administrateur : ces comptes étant membres du domaine, il sera aisé de changer régulièrement leurs mots de passe. Il sera également plus facile de gérer les droits d'accès (ajout, révocation) en modifiant simplement la liste des membres du groupe au niveau du serveur Active Directory.

A noter que l'interdiction d'ouverture de session réseau se fait sur la base d'une liste noire. Dans le cas où d'autres comptes administrateur locaux seraient présents sur les postes, il convient de les rajouter à cette liste afin de leur interdire l'accès distant.

Enfin, afin de rendre plus difficile le « cassage » des mots de passe des comptes locaux, ceux-ci devront respecter des exigences fortes en matière de complexité (cf. Note sur les mots de passe) et l'empreinte LM ne devra pas être générée.

3.2 Interdire la connexion des comptes d'administration de niveau domaine sur les postes utilisateur

Il est important d'interdire techniquement aux comptes ayant des droits d'administration de niveau Active Directory, domaine ou serveurs de s'authentifier sur les postes de travail. En effet, si un compte de ce type était utlisé sur un poste de travail compromis, cela permettrait à un attaquant d'obtenir l'accès aux serveurs et aux postes de travail de l'organisme.

Il convient, dans un premier temps, de créer un groupe utilisateur dans l'Active Directory (par exemple *Groupe-Admins-PDT-Denied*) et de le remplir avec tous les utilisateurs ou groupes ayant des droits d'administration de niveau Active Directory, domaine ou serveurs.

Les membres de ce groupe doivent se voir interdire toute forme d'authentification sur les postes de travail (*Interactive*, *Remote Interactive*, *Network*, *Batch*, *Service*). Cette interdiction doit être mise en oeuvre via une GPO s'appliquant à tous les postes de travail et définissant les paramètres suivants :

- Interdire l'accès à cet ordinateur à partir du réseau
- Interdire l'ouverture d'une session locale
- Interdire l'ouverture de session en tant que service
- Interdire l'ouverture de session en tant que tâche
- Interdire l'ouverture de session par les services Bureau à distance

Documentation

- Recommandation de sécurité relatives aux mots de passe :
  http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf
- Avis CERTA-2013-ACT-017 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-017/

4 Rappel des avis émis

Dans la période du 17 au 22 mai 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-313 : Vulnérabilité dans Cisco TelePresence Supervisor MSE 8050
- CERTA-2013-AVI-314 : Vulnérabilité dans Huawei Quidway
- CERTA-2013-AVI-315 : Vulnérabilité dans Hitachi JP1/Automatic Operation
- CERTA-2013-AVI-316 : Vulnérabilité dans Xen
- CERTA-2013-AVI-317 : Multiples vulnérabilités dans Apple iTunes
- CERTA-2013-AVI-318 : Vulnérabilité dans le système SCADA Schneider
- CERTA-2013-AVI-319 : Vulnérabilité dans EMC RSA SecurID
- CERTA-2013-AVI-320 : Vulnérabilité dans EMC VNX et EMC Celerra Control Station
- CERTA-2013-AVI-321 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-322 : Multiples vulnérabilités dans Moodle
- CERTA-2013-AVI-323 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTA-2013-AVI-324 : Multiples vulnérabilités dans le noyau Linux de Debian

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2013-ALE-005-002 : Vulnérabilité dans le noyau Linux (ajout correctif SUSE)

Gestion détaillée du document

23 mai 2013 version initiale.