Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 janvier 2014
N° CERTA-2014-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2014-ACT-001

1 - Retour d'expérience sur les incidents traités en 2013

Un accroissement des menaces sur les terminaux mobiles

L'utilisation massive, notamment dans les environnements professionnels, d'ordiphones et tablettes tactiles s'est accompagnée d'un accroissement des menaces visant ces périphériques qui contiennent souvent des données très sensibles. Le CERTA tient à rappeler qu'il convient de faire preuve de prudence dans l'utilisation de ces équipements et de respecter les mêmes règles d'hygiène que celles applicables au matériel informatique traditionnel.

Une utilisation accrue de la technique du « point d'eau »

Si le premier vecteur de compromission repose encore sur l'utilisation de courriels malveillants, la technique du « point d'eau » ou « water holing », consistant à introduire une charge malveillante sur un site web vulnérable largement fréquenté par les membres d'une organisation, a été de plus en plus utilisée par les attaquants. La vigilance d'un utilisateur ne se doutant pas de la malveillance d'un site web apparemment de confiance peut alors être mise en défaut.

Le CERTA tient à rappeler que la sécurité d'un système d'information s'appuie aussi bien sur la sécurisation des postes que sur la sensibilisation régulière des utilisateurs.

Des campagnes de courriels malveillants toujours plus fréquentes

Si les menaces évoluent, des attaques pourtant très classiques continuent d'être couronnées de succès. Ainsi en est-il de la diffusion de fichiers malveillants par messagerie. Il pourra s'agir de programmes plus ou moins adroitement dissimulés ou de documents bureautiques (extensions «.pdf», «.doc», «.docx»...) contenant une charge malveillante. Ces incidents pourraient souvent être évités par des mesures simples à mettre en œuvre (sensibilisation des utilisateurs, mesures de filtrage...).

Le CERTA rappelle que les politiques de sécurité doivent impérativement évoluer pour s'adapter aux menaces nouvelles sans omettre les menaces traditionnelles, car les unes comme les autres peuvent mettre en péril le S.I.

Documentation

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

2 - Privilégier l'utilisation du système d'exploitation Windows en 64 bits (deuxième partie)

Depuis Windows Server 2003, Microsoft propose une version 64 bits de ses systèmes d'exploitation, permettant d'utiliser les fonctionnalités de l'architecture x64 des processeurs Intel et AMD (Note : il existe également une version Windows XP 64 bits, mais celle-ci repose en réalité sur un noyau Windows 2003).

Outre l'adressage plus important de la mémoire, un système 64 bits offre plusieurs améliorations en ce qui concerne la sécurité du système.

Le premier article de cette série a présenté les mécanismes ASLR, DEP et la signature des pilotes.

PatchGuard

Le mécanisme de protection contre les modifications en mémoire du noyau Windows baptisé «PatchGuard» est présent uniquement sur les systèmes Windows 64 bits. Afin d'entraver une modification non prévue de structures du noyau, le mécanisme PatchGuard effectue une vérification périodique d'un certain nombre de composants critiques du noyau (couche d'abstraction logicielle, IDT, SSDT, etc.). En cas d'altération non légitime, il provoque alors une extinction du système au travers du Bug Check 0x109 (CRITICAL_STRUCTURE_CORRUPTION).

Sur les aspects purement sécurité, cela permet de se prémunir contre un certain nombre de techniques utilisées par des rootkits en mode noyau pour dissimuler leur présence (technique DKOM pour *Direct Kernel Object Manipulation*) et de dissuader les développeurs contre d'éventuelles modifications affectant la stabilité du système.

Avec Windows 8 ou 2012 en édition 64 bits, PatchGuard surveille davantage d'éléments critiques du noyau.

Abandon de la compatibilité avec les applications 16 bits

Le sous-système MS-DOS (NTVDM) n'est pas présent sur les systèmes 64 bits. Ceci permet de réduire la surface d'exposition (KB2732488, KB937932, KB979682), mais ne permet plus d'exécuter des applications 16 bits.

Points d'attention à prendre en compte lors de l'utilisation d'un système 64 bits

Les produits de sécurité utilisent souvent des techniques nécessitant des modifications non autorisées par PatchGuard et pourront être limités dans leurs fonctionnalités sur les systèmes 64 bits (surveillance des appels système par exemple). C'est pourquoi il faut être vigilant lors de la sélection d'un tel produit et disposer des informations sur la compatibilité de l'outil avec les systèmes 64 bits. Il n'est pas rare que des fonctionnalités mentionnées par l'éditeur ne soient effectivement pas disponibles avec ces systèmes.

Si les applications 32 bits sont censées fonctionner indifféremment sur un système 32 bits ou 64 bits, il n'en est pas de même pour les pilotes noyau. Il est donc nécessaire de s'assurer que le matériel est bien compatible et que des pilotes logiciels existent en version 64 bits pour tous les composants (imprimantes, périphériques externes, etc.).

Choix d'un système

La fin proche du support de Windows XP est souvent l'occasion de réaliser une migration vers Windows 7 ou 8. Au vu des apports en sécurité d'un système Windows 64 bits, il est recommandé de privilégier les versions 64 bits des systèmes Windows. Pour rappel, depuis Windows Server 2008 R2, les architectures 32 bits ont été abandonnées.

3 - Les guides de sécurité 2013 publiés par l'ANSSI

L'ANSSI a publié au cours de l'année 2013 un ensemble de guides de sécurité informatique. L'objectif principal de ces guides est de fournir des recommandations sur les thèmes fondamentaux de la sécurité informatique. Leur application doit permettre de réduire les risques d'intrusion informatique.

Guide d'hygiène informatique

Afin de réduire les risques d'intrusion informatique, il convient pour une organisation de vérifier en priorité qu'elle applique bien les principales règles d'hygiène informatique. Dans cette optique, l'ANSSI a publié un guide comprenant 40 mesures de sécurité.

Les thématiques abordées sont les suivantes :

- connaître le système d'information et ses utilisateurs ;
- maîtriser le réseau ;
- mettre à niveau les logiciels ;
- authentifier l'utilisateur;
- sécuriser les équipements terminaux ;
- sécuriser l'intérieur du réseau ;
- protéger le réseau interne de l'Internet ;
- surveiller les systèmes ;
- sécuriser l'administration du réseau ;
- contrôler l'accès aux locaux et la sécurité physique ;
- organiser la réaction en cas d'incident ;
- sensibiliser ;
- faire auditer la sécurité.

Guide de sécurité BGP

Suite aux études menées par l'observatoire de la résilience de l'Internet français sur la nécessité de sécuriser les interconnexions BGP, l'ANSSI a publié un guide des bonnes pratiques en matière de sécurité sur ce sujet. Les thématiques abordées sont les suivantes :

- sécurité des interconnexions ;
- filtrage des annonces BGP ;
- journalisation.

Des extraits de configurations sont également proposés pour les équipements de marque Alcatel-Lucent, Cisco, Juniper et OpenBGPD.

Guide de sécurité des systèmes industriels

Les systèmes industriels sont de plus en plus souvent interconnectés aux systèmes d'information classiques, voire avec Internet. Ils sont ainsi exposés aux mêmes menaces, mais les risques associés sont généralement plus importants. Dans ce cadre, l'ANSSI a publié un guide sur la cybersécurité de ces systèmes abordant les thématiques suivantes :

- Contexte et enjeux de la cybersécurité des systèmes industriels ;
- Méthode de déploiement de la SSI ;
- Vulnérabilités fréquemment rencontrées ;
- Bonnes pratiques (check-list).

Guide de prévention et bonnes pratiques contre les 0-day

Un 0-Day est une vulnérabilité non corrigée qui peut concerner tout type de logiciel. Ce type de vulnérabilité est susceptible d'être utilisé par des attaquants dans leurs modes opératoires. Afin de s'en prémunir, l'ANSSI a publié un guide de bonnes pratiques répertoriant les actions nécessaires pour renforcer les systèmes d'information face à cette menace. Les thématiques abordées sont les suivantes :

- Définition d'un 0-Day ;
- Sécurité des postes de travail ;
- Sensibilisation de l'utilisateur ;
- Que faire en cas d'incident ;
- Check-List.

Guide de mises en oeuvre d'un système de journalisation

Les journaux sont au coeur du traitement d'incident. Ils permettent de constater rapidement des anomalies, mais également a posteriori de faciliter une éventuelle investigation numérique. Dans cette optique, l'ANSSI a publié une note technique présente des recommandations pour la mise en oeuvre d'un système de journalisation. Les thématiques abordées sont les suivantes :

- prérequis à la mise en place d'un système de journalisation (fonctionnalités, horodatage, synchronisation des horloges, dimensionnement des ressources ...) ;
- architecture et conception (résilience, protection des données échangées, stockage des journaux, consultation des journaux) ;
- types d'évènements à journaliser ;
- aspects juridiques et réglementaires.

Guide de mise en oeuvre d'une politique de restrictions logicielles sous Windows

AppLocker, mécanisme de sécurité disponible depuis Windows 7 et Windows Server 2008, permet de définir des listes blanches de programmes dont l'exécution sera autorisée pour certains utilisateurs en fonction de la politique configurée sur le domaine. Le paramétrage d'AppLocker n'étant pas nécessairement trivial et son utilisation étant fortement recommandée, l'ANSSI a publié un guide pour aider les administrateurs système à le configurer proprement. Les thématiques abordées sont les suivantes :

- Les mécanismes SRP et AppLocker ;
- Mise en oeuvre d'une stratégie de restrictions logicielles avec AppLocker ;
- Considérations de sécurité fondamentales.

Documentation

- Guide d'hygiène informatique :
  http://www.ssi.gouv.fr/hygiene-informatique
- Guide des bonnes pratiques de sécurisation BGP :
  http://www.ssi.gouv.fr/bonnes-pratiques-bgp
- Guide de sécurisation des systèmes industriels :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-systemes-industriels/la-cybersecurite-des-systemes-industriels.html
- Guide de mises en oeuvre d'un système de journalisation :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/vulnerabilites-0-day-prevention-et-bonnes-pratiques.html
- Guide de mise en oeuvre d'une politique de restrictions logicielles sous Windows :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-de-securite-pour-la-mise-en-oeuvre-d-un-systeme-de.html

4 - Rappel des avis émis

Dans la période du 27 décembre 2013 au 02 janvier 2014, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-687 : Multiples vulnérabilités dans Puppet
- CERTA-2014-AVI-001 : Multiples vulnérabilités dans les équipements Huawei

Gestion détaillée du document

03 janvier 2014 version initiale.