Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 24 juillet 2017
N° CERTFR-2017-ACT-029

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-029

1 - Mouvements latéraux et cloisonnement

Contexte

Les récentes vagues de rançongiciel se sont propagées au sein de systèmes d'information, au moyen de techniques de déplacement latéral dans un même réseau Microsoft Windows, occasionnant des dégâts qui peuvent toutefois être contenus si une stratégie de cloisonnement système et réseau appropriée est appliquée.

Ces mouvements latéraux sont souvent effectués :

- en utilisant des identifiants récupérés sur une machine compromise pour se connecter à une machine du même réseau Microsoft Windows (ex. : *NotPetya*) ;
- en exploitant une vulnérabilité présente sur plusieurs machines du même réseau Microsoft Windows (ex. : MS17-010 pour *NotPetya* et *Wannacry*).

Le rançongiciel *NotPetya* utilisant les deux méthodes, la propagation au sein d'un même système d'information a été d'autant plus importante.

Les recommandations ci-dessous sont des éléments permettant de réaliser un cloisonnement réseau et système efficace. Ces mesures viennent en complément des bonnes pratiques générales de sécurité à appliquer sur un système d'information.

Recommandations

Pour réaliser un cloisonnement efficace du système d'information, il convient avant tout de classer les machines en différentes familles. Voici les différents types de machines que l'on peut souvent identifier au sein d'un réseau Microsoft Windows :

Les postes des utilisateurs

- Cloisonnement réseau :
  1. Ces postes utilisateurs se situent dans un segment réseau dédié et un filtrage de flux approprié est réalisé avec les autres segments du système d'information.
  2. Souvent les postes utilisateurs n'ont pas besoin de communiquer entre eux sur le même segment réseau ; si c'est le cas, utiliser la fonctionnalité *Private VLAN* (ou isolation de ports) du commutateur réseau sur ce segment réseau. Cela empêche les postes de communiquer entre eux, donc le mouvement latéral au sein de ce segment.
  3. Il est aussi possible de bloquer toutes les connexions entrantes venant de ce segment réseau via le pare-feu local Microsoft Windows du poste utilisateur. Celui-ci est configurable via GPO.

– Cloisonnement système :
    1. Les utilisateurs du système d'information ont des comptes de domaine Active Directory qui ne sont pas administrateur local du poste de travail.
    2. Les comptes Active Directory utilisés pour l'administration des postes utilisateurs sont dédiés à cet usage et ne peuvent gérer que ces derniers.
    3. Les comptes d'administration locaux sont gérés avec *LAPS* (*Local Administrator Password Solution*) et ne peuvent pas ouvrir de session de type réseau (type 3).

Les serveurs applicatifs

– Cloisonnement réseau :
    1. Ces serveurs se situent *a minima* dans un segment réseau dédié, et un filtrage de flux approprié est réalisé avec les autres segments du système d'information.
    2. Si possible, regrouper ces serveurs par type (ex. : "Présentation Web", "Base de données"...) et sensibilité au sens métier dans des segments réseaux dédiés et leur appliquer un filtrage de flux approprié.
– Cloisonnement système :
    1. Les comptes d'administration Active Directory utilisés pour la gestion des serveurs applicatifs sont dédiés à cet usage et ne peuvent gérer que ces derniers.
    2. Les comptes d'administration locaux sont gérés avec *LAPS* (*Local Administrator Password Solution*) et ne peuvent pas ouvrir de session de type réseau (type 3).
    3. Si la virtualisation est utilisée : regrouper si possible les serveurs de même type et même sensibilité au sens métier sur les mêmes hyperviseurs.

Les contrôleurs de domaine

– Cloisonnement réseau :
    1. Ces serveurs se situent dans un segment réseau dédié et un filtrage de flux approprié est réalisé avec les autres segments du système d'information.
    2. Ces serveurs n'ont pas accès à Internet, même au travers d'un serveur mandataire.
– Cloisonnement système :
    1. Les comptes administrateur du domaine Active Directory utilisés pour la gestion des contrôleurs de domaine ne peuvent gérer que ces derniers.
    2. Aucun autre rôle système n'est installé sur ces serveurs (serveur Web par exemple).
    3. Si la virtualisation est utilisée : regrouper si possible les contrôleurs de domaine sur les mêmes hyperviseurs.

Un administrateur de réseau Microsoft Windows peut donc posséder jusqu'à quatre comptes : un compte utilisateur standard qu'il utilisera pour consulter ses courriels et naviguer sur Internet depuis son poste utilisateur, et trois comptes qu'il utilisera pour administrer les trois familles de machines mentionnées plus haut, ceci depuis une console d'administration qui sera située dans un segment réseau dédié n'ayant pas accès à Internet, même au travers d'un serveur mandataire.

Documentation

– Gestion des mots de passe administrateurs locaux *LAPS* :
http://cert.ssi.gouv.fr/site/CERTFR-2016-ACT-008/
– Bloquer l'ouverture de session de type réseau (type 3) des comptes administrateurs locaux :
https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/
– Recommandations de sécurité relatives à Active Directory :
https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/
– SSTIC 2017 l'administration en silo :
https://www.sstic.org/2017/presentation/administration_en_silo/
– Investigation numérique, identifier les traces de mouvement latéraux :
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-037/CERTFR-2014-ACT-037.html
http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-038/CERTFR-2014-ACT-038.html

2 - Rappel des avis émis

Dans la période du 17 au 23 juillet 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-217 : Multiples vulnérabilités dans le noyau Linux de SUSE
- CERTFR-2017-AVI-218 : Multiples vulnérabilités dans Apache
- CERTFR-2017-AVI-219 : Multiples vulnérabilités dans SCADA Siemens Android App SIMATIC Sm@rtClient
- CERTFR-2017-AVI-220 : Multiples vulnérabilités dans Moodle
- CERTFR-2017-AVI-221 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2017-AVI-222 : Multiples vulnérabilités dans Wireshark
- CERTFR-2017-AVI-223 : Multiples vulnérabilités dans Oracle Java SE
- CERTFR-2017-AVI-224 : Multiples vulnérabilités dans Oracle MySQL
- CERTFR-2017-AVI-225 : Multiples vulnérabilités dans Oracle Linux and Virtualization
- CERTFR-2017-AVI-226 : Multiples vulnérabilités dans Oracle Database Server
- CERTFR-2017-AVI-227 : Multiples vulnérabilités dans Oracle Sun Systems Products Suite
- CERTFR-2017-AVI-228 : Multiples vulnérabilités dans SCADA Schneider Electric Trio TView
- CERTFR-2017-AVI-229 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2017-AVI-230 : Vulnérabilité dans Cisco Web Security Appliance
- CERTFR-2017-AVI-231 : Multiples vulnérabilités dans Oracle VM Server pour x86 et Oracle Linux
- CERTFR-2017-AVI-232 : Vulnérabilité dans le noyau Linux de SUSE
- CERTFR-2017-AVI-233 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

24 juillet 2017 version initiale.