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 23 mai 2016
N° CERTFR-2016-ACT-021

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-021

1 - Risques associés aux NAS

La sécurité des serveurs de stockage en réseau

Un serveur de stockage en réseau, connu également sous le nom de "NAS" (du nom anglais "Network Area Storage"), est un équipement réseau proposant principalement un service de partage de fichiers pour l'ensemble des ordinateurs autorisés. L'accès aux données est généralement réalisé par des protocoles standards : SMB, NFS, AFP, FTP, WebDAV, etc.

Ce type d'équipement peut offrir de nombreux autres services réseau : serveur DHCP, serveur de sauvegarde, centralisation de journaux d'événements (syslog), serveur de messagerie, serveur multimédia, serveur de VPN, etc. Autant de fonctionnalités qui augmentent l'exposition de l'équipement à une vulnérabilité. Il est donc impératif de :

- sécuriser l'accès réseau au serveur et l'accès logique aux données ;
- sauvegarder les données ;
- mettre à jour le logiciel de gestion du serveur.

Exposition depuis des réseaux externes

Il convient de n'autoriser que les connexions nécessaires au serveur, en particulier venant de réseaux externes. Cela se configure dans la passerelle Internet et/ou le pare-feu (réacheminement de ports, routage d'adresses, ...), ainsi que dans la configuration du serveur de stockage en réseau (accès externe).

Le principe de défense en profondeur doit être appliqué et la configuration des différents équipements réseau doit être durcie.

Accès aux données

Les fichiers présents sur cet équipement étant accessibles depuis toutes les machines du réseau, il est important de protéger leur accès par l'utilisation d'identifiants distincts pour chaque utilisateur et de mots de passe forts.

En plus de l'authentification des connexions, il faut mettre en place des permissions garantissant que seuls les accès légitimes sont possibles. Cela limite également l'exposition des informations aux rançongiciels. De tels maliciels, lorsqu'ils s'exécutent, chiffrent tous les fichiers accessibles, depuis la machine où ils s'exécutent, qu'ils soient locaux ou distants.

Sauvegarde des données

La sauvegarde des données sur un support déconnecté est l'une des dix règles de base de la sécurité. C'est l'élément indispensable afin de pouvoir réagir à une attaque (rançongiciel par exemple) ou un dysfonctionnement (suppression accidentelle ou panne matérielle).

Maliciels spécifiques

Il est à noter l'existence de programmes malveillants destinés spécifiquement aux serveurs de stockage en réseau. Le plus connu est nommé Synolocker, apparu en 2014, qui ciblait les équipements de la marque Synology.

Mises à jour

Comme pour tout équipement informatique, des failles peuvent exister dans son système d'exploitation ou dans les composants logiciels qu'il exécute. Lorsque de tels risques de sécurité sont identifiés, les éditeurs publient des mises à jour corrigeant la ou les vulnérabilités. Comme pour tout système, il faut s'assurer que celui-ci est bien maintenu à jour.

Responsabilités

En matière de responsabilité pénale et de risque juridique, les gestionnaires / responsables de systèmes connectés doivent globalement être attentifs tant aux risques touchant aux contenus qu'à ceux liés à la bande passante ou connectivité du système concerné :

- les risques liés aux contenus illégaux qui sont récurrents sur ces espaces de stockage en ligne (pédopornographie, infraction aux droits d'auteur - musique - jeux - films) ;
- les risques liés à l'utilisation du système ou de sa connectivité à l'Internet pour être utilisés comme rebond / relais afin de commettre des infractions sur des serveurs tiers.

Références

- Sécurité des mots de passe :
  http://www.ssi.gouv.fr/guide/mot-de-passe/
- Dix règles de base :
  http://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/
- Synolocker :
  https://www.symantec.com/security_response/writeup.jsp?docid=2014-080708-1950-99

2 - Rappel des avis émis

Dans la période du 16 au 22 mai 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-171 : Multiples vulnérabilités dans le noyau d'Ubuntu
- CERTFR-2016-AVI-172 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2016-AVI-173 : Vulnérabilité dans le moteur Antivirus Symantec
- CERTFR-2016-AVI-174 : Multiples vulnérabilités dans Moodle
- CERTFR-2016-AVI-175 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-176 : Vulnérabilité dans Xen
- CERTFR-2016-AVI-177 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-178 : Multiples vulnérabilités dans SCADA Siemens SIPROTEC 4 et SIPROTEC Compact

Gestion détaillée du document

23 mai 2016 version initiale.