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 08 août 2016
N° CERTFR-2016-ACT-032

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-032

1 - Rappel autour des sauvegardes

Les sauvegardes de données sont des éléments critiques des systèmes d'information. Elles permettent, en cas de perte de données, leur restauration. La stratégie de sauvegarde d'une entreprise s'inscrit dans une démarche plus large de plan de continuité d'activité qui considère tous les événements pouvant interrompre la bonne marche de l'entreprise (perte d'information, mais également catastrophe naturelle, conflit, etc.).

La stratégie de sauvegarde de l'entreprise définit :

- les scénarios de perte d'information à couvrir (panne matérielle, suppression accidentelle, acte de malveillance incluant les rançongiciels, sinistre) ;
- les données à sauvegarder (informations crées par l'entreprise, configuration de système, annuaire d'entreprise, etc.) ;
- la fréquence de sauvegarde (quotidienne, hebdomadaire, etc.) ;
- la durée de rétention souhaitée et le nombre de versions à conserver ;
- les procédures de sauvegarde et de restauration ;
- les personnes responsables des différentes phases (mise en oeuvre, vérification, etc.).

À partir de ces éléments stratégiques, il faudra identifier les solutions pratiques à mettre en oeuvre en considérant des paramètres comme le volume à sauvegarder et à conserver, la vitesse de transfert, la durée de sauvegarde et le coût.

Les sauvegardes peuvent être réalisées vers des supports physiques (bandes magnétiques, disque dur externe, clé USB), sur un serveur dédié, ce dernier pouvant se trouver sur un autre site géographique pour une reprise en cas de sinistre local, ou sur Internet (solutions en ligne).

Une fois le plan de sauvegarde défini et rédigé, il doit être revu et testé à intervalle régulier pour s'assurer qu'il est à jour. Un changement de version de l'outil, une réorganisation interne ou un équipement défectueux seront ainsi identifiés et la procédure modifiée en conséquence.

Les systèmes d'information actuels contiennent désormais d'autres équipements que des ordinateurs. Tous les appareils de mobilité (tablettes et ordiphones) connectés au réseau d'entreprise peuvent contenir des informations de valeurs et sont susceptibles d'être perdus ou volés. Il est donc impératif d'inclure ces équipements dans la stratégie de sauvegarde en place dans l'entreprise.

En conclusion, la définition d'un plan de sauvegarde est un projet complet. Il doit définir précisément ce qui doit être sauvegardé, quand, par qui et comment.

Documentation

- Guide des bonnes pratiques de l'informatique (chapitre 4/ Effectuer des sauvegardes régulières) : http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/
- Bulletin d'actualité CERTFR-2014-ACT-039 (section 3 - Sauvegardes des données mobiles et risques) : http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-039

2 - Rappel des avis émis

Dans la période du 01 au 07 août 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-256 : Multiples vulnérabilités dans Nagios
- CERTFR-2016-AVI-257 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-258 : Vulnérabilité dans SCADA Siemens Sinema Server
- CERTFR-2016-AVI-259 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-260 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-261 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-262 : Multiples vulnérabilités dans les pilotes de noyau Linux de NVIDIA Tegra
- CERTFR-2016-AVI-263 : Vulnérabilité dans LibreOffice
- CERTFR-2016-AVI-264 : Vulnérabilité dans Apple iOS
- CERTFR-2016-AVI-265 : Multiples vulnérabilités dans les produits VMware

Gestion détaillée du document

08 août 2016 version initiale.