Politiques de sauvegardes

Octobre 2017 - Mois européen de la cybersécurité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

TABLE DES MATIERES

MENACES

Depuis 2015, les rançongiciels ont constitué des tests majeurs pour la sécurité des systèmes d'information. **Le scénario catastrophe se matérialise lorsque l'irruption d'un rançongiciel se combine avec un échec non détecté de sauvegardes empêchant le recouvrement de données.**

Des pertes d'exploitation importantes ont été constatées, y compris dans de grandes organisations, lorsque les logiciels malveillants se sont implantés sur des infrastructures mal préparées, avec blocages d'équipes entières pendant plusieurs semaines, et des impacts durables pendant une longue période.

Outre les logiciels malveillants, la préparation à la résilience des systèmes ne doit pas perdre de vue les corruptions des supports, du système de sauvegardes lui-même ou des erreurs de manipulation. Par exemple, les taux d'erreur matériel (i.e. nombre de bits non-relus sur un support magnétique) ne connaissent plus d'évolution significative (ou les courbes de défaillance prennent une forme très différente, avec les SSD), si bien qu'avec l'augmentation des volumes de données, il n'est pas rare que les méthodes suffisantes dans les années 2000 montrent des défaillances.

ETAT DE L'ART

Politique 3-2-1

Une politique de sauvegardes « 3-2-1 » est une appellation mnémonique (cf. [1] à [3]) pour un système basé sur les principes suivants :

- **3 copies** au moins des données protégées, les données primaires et deux sauvegardes
- **2 médias & systèmes**, parce que chaque support (disque dur / bande) ou système (SAN / NAS) peut être un point de défaillance unique ; la première sauvegarde se trouve sur site, pour une capacité de reconstruction rapide.
- **1 site externe** pour la deuxième sauvegarde afin de disposer d'une ressource ultime, même si un événement catastrophique touchait le premier site.

Si le nom est facile à mémoriser, la mise en œuvre demande du soin pour éviter des « découvertes douloureuses » comme :

- des ensembles RAID ne constituent pas un original et une copie de sauvegarde, même en mode miroir ; des ensembles RAID forment un procédé qui améliore la disponibilité et les performances en lecture mais les défaillances de disques ne sont pas indépendantes (en particulier pour les systèmes à parité qui sollicitent soudainement et fortement les disques quand un premier disque est détecté comme défaillant).
- les sauvegardes chaînées (original, sauvegarde sur site, sauvegarde hors site) sans contrôle d'intégrité à chaque étape ne font que propager les erreurs.

Vérifications d'intégrité et notifications

Autrement dit, une copie simple de fichiers n'est pas un système de sauvegardes professionnel. L'état de l'art comprend :

- utilisation de sommes de contrôle pour vérifier que la copie est intègre ;
- notification des erreurs mais aussi des « succès », avec le volume de données sauvegardées, jusqu'à un administrateur système (éventuellement via un système de supervision capable d'analyser, synthétiser).

Sauvegarde différentielle avec déduplication

Aujourd'hui un attaquant a tendance à chiffrer ou corrompre les données en masse. Les systèmes de détection s'adaptant, il est probable que les attaquants modifient leurs tactiques pour reproduire celles des corruptions matérielles, beaucoup plus lentes.
Dans tous les cas, la seule protection face à ces corruptions lentes consiste à disposer d'une « profondeur » d'historique de sauvegardes également longue, jusqu'à 1 an. Avec des approches traditionnelles de copies intégrales de répertoires, cette durée de rétention conduit rapidement à des volumes importants. Mais l'état de l'art consiste à utiliser pleinement les sauvegardes différentielles (uniquement les nouveaux fichiers) et la déduplication (uniquement les blocs modifiés). Comme l'expérience montre que les données « froides » (à peine lues de temps en temps) sont beaucoup plus volumineuses que les données « chaudes » (en modification rapide), un ajout de 50% de capacité suffit généralement à prolonger les archives de sauvegardes sur au moins un an.

Chiffrement par la source

Une politique de sauvegardes hors site primaire et une durée de rétention longue a pour conséquence d'augmenter le risque d'exposition des données.
Dès lors, l'état de l'art s'est adapté en adoptant la pratique de chiffrement des données par la source. Ainsi la protection des données est ramenée à la gestion du secret aléatoire utilisé pour chiffrer les sauvegardes.

RECOMMANDATIONS PRATIQUES

Outre les solutions traditionnelles d'éditeurs (dont celui expliquant la politique 3-2-1 dans [1]) ou open source [4], les cinq dernières années ont vu fleurir de nombreuses solutions Open Source, répondant aux nouvelles pratiques de l'état de l'art, disponibles sur toutes plateformes Windows/Linux/macOS ([5] à [11] par exemple).

Si l'organisation ne possède pas plusieurs sites équipés d'infrastructures informatiques, les sauvegardes « dans les nuages » permettent de disposer de toute la capacité nécessaire pour les copies distantes, du moment que les données sont chiffrées avec une clé géré par l'organisation (condition *sine qua non* sous peine de graves compromissions de données) ; les prestataires spécialisés permettent de recevoir par la Poste un disque externe pour rapatrier de gros volumes de données en cas d'incident car les accès réseaux habituels sont généralement insuffisants.

Formaliser la politique de sauvegardes

Les obstacles à des sauvegardes systématiques ne sont donc pas ni la faisabilité, ni la disponibilité des technologies mais un manque d'organisation opérationnelle. C'est pourquoi la première étape pour une entreprise ou organisation, consiste à formaliser une politique de sauvegardes standardisée. Cette politique indique les moyens et garanties apportées par la politique de sauvegardes :

- **protection contre les défaillances de sites ou de supports** : plan de sauvegardes « 3-2-1 »
- **protection contre les corruptions techniques** : contrôle d'intégrité et notification
- **protection contre les corruptions lentes** : historique sur plusieurs mois
- **protection contre les divulgations de données par l'accès aux sauvegardes** : chiffrement par la source
- **protection contre les erreurs de manipulation des utilisateurs** : réduction du délai entre sauvegardes successives (de 1j à 1h pour les espaces de documents) et historisation « d'instantanés »

Si elle n'est pas déjà à l'état de l'art, la politique peut déboucher et renvoyer à un plan d'actions permettant de combler le retard**.**

La politique de l'organisation précise la fréquence des sauvegardes, et spécifie ses champs d'application. D'une manière générique, elle a vocation à inclure :

- *toutes données créées ou compilées par l'organisation*
- espaces de fichiers servant de bases de documents
- bases de données structurées (fichier global ou export SQL)
- configurations ou machines virtuelles, dès lors qu'elles forment une unité fonctionnelle dont la défaillance conduirait à un déni de service incompatible avec l'objectif de disponibilité, du fait d'une attaque et d'une tentative d'extorsion ou pour toute autre raison.

Le champ d'application de la politique de sauvegardes peut exclure :

- toutes les données dont l'exclusion de couverture est clairement identifiée aux utilisateurs

- par exemple, disque complet des postes de travail, serveurs ou ordiphones (car trop d'éléments communs, de cache temporaire, même si la déduplication limite l'impact), lorsque les collaborateurs sont invités à utiliser des espaces partagés

Elaborer le plan de maintenance

Même avec des systèmes de stockage conçus pour supporter une politique bien conçue, la disponibilité des sauvegardes en cas de besoin peut aussi être défaillante par manque de maintenance. De plus, dans l'affolement d'un incident, il est préférable d'avoir rodé la restauration de données à partir des sauvegardes.

L'automatisation est le premier niveau de réponse. Mais comme l'ont démontré un certain nombre de catastrophes, encore faut-il que **quelqu'un s'assure que l'automatisme** fonctionne et n'est pas bloqué par exemple par la saturation des espaces de stockages.

A ce deuxième niveau, la méthode la plus sûre contre ces défaillances consiste à **« arrimer » le plan de sauvegardes aux processus déjà en place de vérification et d'exercice de l'organisation** : certification qualité ISO, revues mensuelles / trimestrielles de tableaux de bord de la production informatique, etc. Une autre variante, mnémotechnique, consiste à faire un exercice de restauration de données systématiquement la semaine qui suit un exercice d'évacuation incendie (obligation légale de les faire tous les 6 mois).

Ces automatismes et arrimages sont à mentionner explicitement dans la politique de sauvegardes.

EN RESUME

Une politique de sauvegarde est le premier rempart pour la résilience des systèmes d'information. En étant synthétique, une politique de sauvegardes, plan de maintenance inclus, tient sur une page A4.

La formalisation au sein d'une organisation constitue la première étape pour une maîtrise raisonnée, d'autant que les moyens techniques à mettre en œuvre sont bien moins couteux que ce qu'ils n'étaient il y a 10 ou 20 ans.
L'automatisation puis les processus de l'organisation et son management doivent ensuite permettre que la mise en œuvre effective de la politique de sauvegardes soit aussi régulière que la maintenance des ascenseurs ou les exercices d'évacuation.

RÉFÉRENCES

[1] https://www.veeam.com/blog/fr/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html
[2] https://www.backblaze.com/blog/the-3-2-1-backup-strategy/

[3] http://dpbestflow.org/node/262
[4] http://blog.bacula.org/
[5] https://restic.github.io/
[6] http://duplicity.nongnu.org/
[7] http://www.duplicati.com/
[8] http://mattmahoney.net/dc/zpaq.html en particulier dans des environnements Windows
[9] http://zbackup.org/
[10] https://attic-backup.org/
[11] https://github.com/borgbackup/borg

Contact : dssi.shfds (at) finances.gouv.fr
Diffusion Internet : https://www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

HFDS Bercy