Journalisation : les 14 nouvelles recommandations de l'ANSSI

Quelle mesures de sécurité pour un système de journalisation ? L'ANSSI avait publié, fin 2013, une note technique à ce sujet. Elle vient de l'actualiser. Aux 17 recommandations initiales viennent s'en ajouter 14. Les voici.

1 – Activer la journalisation sur un nombre important d'équipements du SI

En commençant par ceux qui composent les passerelles Internet sécurisées et par ceux qui supportent les valeurs métiers les plus importantes ou qui disposent d'un chemin de contrôle permettant d'accéder à ces données.

2 – Homogénéiser les paramètres d'horodatage

Cette recommandation complète celle invitant à activer l'horodatage pour l'ensemble des événements. Homogénéiser, c'est notamment avoir un fuseau horaire de référence et synchroniser les horloges avec une précision minimale à la seconde.

3 – Identifier la granularité de journalisation des équipements

Pour chaque équipement, sélectionner les types d'événements devant être stockés. Une politique qui prend en compte les capacités de stockage, de collecte et de traitement des événements. Ainsi que les besoins de sécurité de l'équipement.

4 – Journaliser les empreintes des fichiers potentiellement malveillants

5 – Contrôler régulièrement la couverture de la chaîne de collecte des événements

En d'autres termes, tester régulièrement que tous les systèmes du SI sont bien journalisés (hors exception dûment identifiées). Et qu'ils transfèrent leurs événements à des serveurs de collecte des journaux.

Journalisation : *pull* ou *push* ?

6 – Adopter un transfert des journaux en temps différé

On choisira cette option à défaut de pouvoir effectuer un transfert « temps réel ». L'envoi des journaux aux serveurs de collecte se fera alors « au plus tard quelques heures après leur génération ».

7 – Faire une analyse de risque pour déterminer le mode de transfert des journaux

Pull ou *push* ? Cela doit se décider au cas par cas. En fonction du niveau de sensibilité du serveur collecté et du collecteur. Ainsi que de la surface d'attaque qu'induit la solution retenue. Le mode push authentifié, par exemple, ouvre la voie aux attaques par relais d'authentification, tout en augmentant la surface d'attaque des serveurs centraux. Le mode pull peut nécessiter un compte de service disposant de droits d'authentification sur de nombreuses ressources du SI. On pourra minimiser les risques par filtrage d'IP, en forçant l'authentification par Kerberos ou encore en changeant régulièrement le mot de passe du compte de service.

8 – Privilégier le stockage des journaux dans une base de données indexée

Si cela n'est pas possible, on stockera les journaux d'événements dans une arborescence de répertoires classés par thématiques (authentification, applications métiers, web…).

9 – Restreindre au strict besoin opérationnel les droits de suppression des journaux

Faire en sorte que seuls les comptes utilisateurs dédiés à l'administration privilégiée des équipements disposent de ces droits. Cette recommandation complète celle applicable aux droits d'accès en écriture.

10 – Restreindre au strict besoin opérationnel les droits d'accès en lecture aux journaux

En cas d'externalisation…

11 – Étudier l'alternative d'un ou plusieurs systèmes de journalisation

Cela suppose d'évaluer les prestataires sur leur capacité à générer des journaux sur les solutions retenues, à les stocker de manière sécurisée et à les rendre disponibles pour le client. Ainsi que leur capacité à s'interconnecter au niveau réseau et à synchroniser la source de temps sur une horloge interne à l'entité. À examiner aussi : la facturation de la bande passante sortante en prévision d'un éventuel export.

12 – Récupérer les journaux relatifs aux interconnexions

En cas d'externalisation d'un sous-système du SI de l'entité, récupérer, de préférence sur le système de journalisation interne de l'entité, tous les journaux liés à l'interconnexion (concentrateurs VPN, serveurs de fédération d'identité…).

13 – Recourir à un PDIS (prestataire de détection des incidents de sécurité) en en cas d'externalisation du stockage ou de la corrélation de journaux

14 – Collecter les journaux des postes en situation de nomadisme

Qu'en est-il si le poste de travail ne peut pas joindre un serveur de collecte pendant une certaine durée alors qu'il est connecté au SI ? S'il existe, configurer le système de détection d'incidents pour

déclencher des alarmes.
Lorsque la centralisation à travers un tunnel VPN est impossible et qu'un système se trouve déconnecté pour une durée moyenne à longue, la centralisation de ses événements perd son intérêt. Il est dans ce cas nécessaire d'envisager d'autres stratégies de sécurisation et de supervision.

Illustration principale © Pavel Ignatov – Adobe Stock