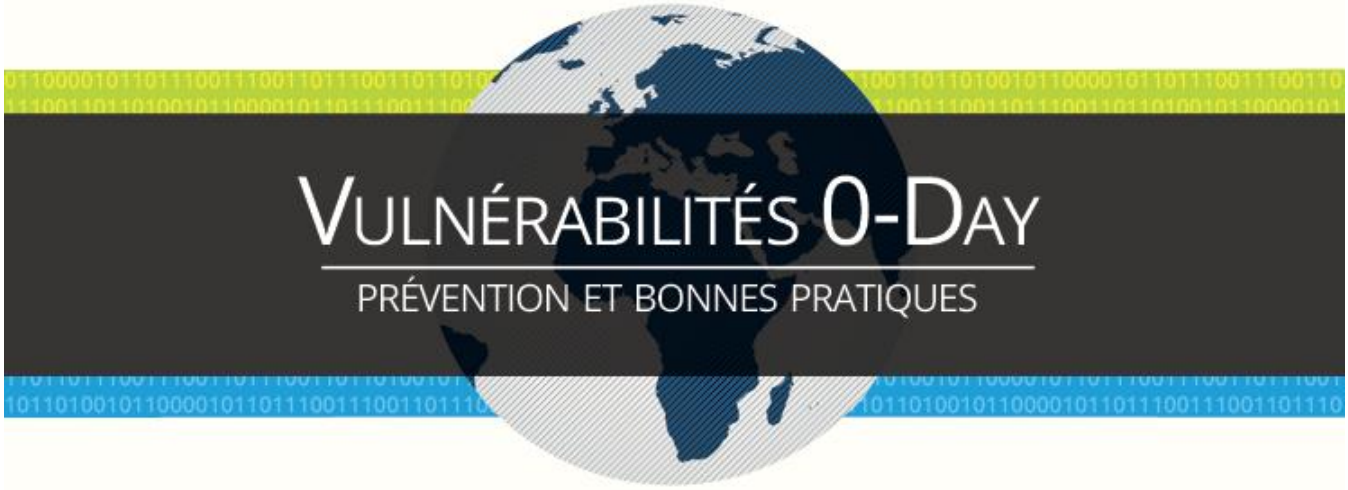
Public : **DSI et ★RSSI**



VULNÉRABILITÉS 0-DAY

PRÉVENTION ET BONNES PRATIQUES

www.ssi.gouv.fr

ANSSI

À propos de l'ANSSI

L'Agence nationale de sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.
En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n°2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétariat général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

Pour en savoir plus sur l'ANSSI et ses missions, rendez-vous sur www.ssi.gouv.fr

AVANT-PROPOS

Ce document rédigé par l'agence nationale de la sécurité des systèmes d'information (ANSSI) présente des recommandations de sécurité relatives à la prévention des 0-days.

Il est téléchargeable sur le site http://www.ssi.gouv.fr.

il constitue une production originale de l'anssi placée sous le régime de la licence ouverte publiée par la mission Étalab (www.etalab.gouv.fr). Il est diffusable sans restriction.

L'ANSSI attire votre attention sur la nécessité de disposer de systèmes et logiciels mis à jour régulièrement, car de nombreuses attaques se font par le biais de vulnérabilités connues de longue date.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être utilisées sans adaptation sur les systèmes cibles.

Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit etre soumise à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

> **! Mesures d'hygiène informatique**
>
> **Si les attaques par 0-Day représentent un risque important, les organisations sont exposées à de nombreux autres risques, pour certains plus élémentaires. Il convient pour une organisation de vérifier en priorité qu'elle applique bien les principales règles d'hygiène informatique.**
>
> **Le Guide d'hygiène informatique publié en janvier 2013 par l'ANSSI est disponible en ligne : http://www.ssi.gouv.fr/hygiene-informatique**

0-DAY - DÉFINITION

UN 0-DAY EST UNE VULNÉRABILITÉ NON-CORRIGÉE DANS UN CODE LOGICIEL.

- **Cette vulnérabilité peut permettre l'exécution de codes arbitraires ou le contournement de politiques de sécurité.**

Un 0-Day peut concerner tout type de logiciel (suite bureautique, application métier, système d'exploitation, logiciel embarqué, application mobile etc.).

Le terme *« 0-Day »* est employé en référence au temps théoriquement très court qui sépare la découverte de la vulnérabilité et son exploitation par un attaquant à titre offensif avant le développement d'un correctif. Si les CERT et les éditeurs cherchent à avoir connaissance des vulnérabilités et à développer des correctifs aussi rapidement que possible, le délai – même très court entre la publication de la vulnérabilité, la publication et l'application du correctif – peut néanmoins permettre à des attaquants d'exploiter ces failles.

- **Les 0-Days constituent un risque majeur et permanent pour les systèmes d'information.**

- **Les conséquences de l'exploitation par un attaquant d'un 0-Day peuvent être très lourdes : indisponibilité du système concerné, intrusion, vol de données, etc.**

- **Dans la plupart des cas, l'image de marque envers des utilisateurs ou clients du service sera dégradée, et des pertes financières seront constatées (au minimum coût financier pour les opérations non réalisées du fait des indisponibilités, coût humain rendu nécessaire par la restauration du système dans l'urgence, etc.).**

Pourtant, les attaques par 0-Day ne sont pas une fatalité : en les anticipant on peut s'en prémunir, ou du moins limiter leur impact.

SÉCURITÉ DES POSTES DE TRAVAIL

La prévention du 0-Day nécessite la mise en œuvre d'un cercle vertueux de bonnes pratiques pour limiter la surface d'exposition aux vulnérabilités.

La liste suivante contient des conseils destinés à vous aider à vérifier et renforcer la sécurité des postes de travail, des serveurs et de vos réseaux étape par étape *(un schéma est disponible en dernière page)*

- **Adoption d'un parc matériel et logiciel homogène**.
  La gestion quotidienne est simplifiée et les mises à jour sont facilitées.

  ★ **En mode avancé,** prévoir une redondance du réseau avec des logiciels et des équipements de nature différente ; voir Points 8 et 9.

- **Séparation des profils administrateurs et utilisateurs pour un même poste suivant une logique de restriction des privilèges.**
  La suppression des droits d'administration aux utilisateurs classiques et l'application de restrictions d'exécution des applications limitent la capacité de nuisance de l'attaquant. Par ailleurs, l'interdiction pour les comptes d'administration d'avoir accès à internet ou à la messagerie constitue un obstacle important à la propagation des attaques informatiques dans un réseau.

- **Désactivation de toutes les extensions (greffons) inutiles**.

  ★ Pour les navigateurs, il faut s'assurer de la désactivation des greffons inutiles, et des *handlers* (appel du navigateur à des logiciels tiers)

  Des extensions de navigateurs permettent de bloquer l'exécution automatique des logiciels tiers tels que Flash (*flashblock* pour Firefox ou *Click-to-play* pour Google Chrome). D'autres permettent de gérer la politique d'exécution des contenus actifs (*noscript* pour Firefox ou *scriptsafe* pour Google Chrome).

  ★ Il est de plus recommandé de réduire au maximum la « surface d'exposition », en désactivant les services inutiles des applications métier et des systèmes d'exploitation afin de réduire les vecteurs d'attaques.

- **Mise à jour régulière des logiciels et systèmes**.
  Les mises à jour permettent de diminuer la fenêtre de vulnérabilité liée à la présence de vulnérabilités connues.

Mise en œuvre de mécanismes de durcissement générique pour complexifier l'exploitation de vulnérabilités.

- Ne pas omettre de déployer des outils comme *EMET* en environnement Windows, ou encore *Grsecurity, SELinux* ou tout autre mécanisme de durcissement et de renforcement du contrôle d'accès en environnement Linux.

Renfort de la sécurité périmétrique, bonne configuration des pare-feux.

La configuration restrictive du pare-feu permet de limiter l'exposition aux vulnérabilités.

Analyse des journaux et supervision.

La mise en place d'une journalisation et l'exploitation des journaux du proxy et du pare-feu permettent de détecter plus rapidement un incident et d'y remédier.

Identification des modes dégradés.

Le passage en mode dégradé doit faire l'objet d'une procédure d'aide à la décision, qui prendra en compte :

- Le temps de réaction aux incidents ;

- l'impact prévisible sur le réseau, les machines, les logiciels et les applications métier, ainsi que sur les utilisateurs finaux.

Mise en place d'une redondance de l'architecture du SI.

- La redondance de l'architecture SI permet la bascule rapide de tout le réseau en cas de détection d'anomalie. Elle doit être prise en compte dans les plans de continuité d'activité. Elle participe indirectement à améliorer les capacités de réaction en cas d'exploitation de 0-Day sur le réseau.

Mise à disposition de plusieurs navigateurs.

Le navigateur Web, interface très utilisée et très exposée, est susceptible de donner accès à des ressources internes à des personnes non autorisées. Les navigateurs sont une cible particulièrement attrayante pour les attaquants.

L'installation de deux navigateurs web différents facilite une bascule de l'un vers l'autre en cas de détection de vulnérabilité ou de dégradation du fonctionnement. Pour que cette mesure soit efficace, les deux navigateurs doivent systématiquement être à jour de tous leurs correctifs de sécurité.

- Pour accompagner cette mesure, il faut pouvoir informer rapidement les utilisateurs de changer de navigateur principal et filtrer les *« user-agent »* au niveau du proxy.

- De plus, il est préférable d'intégrer dans les règles de conception et les cahiers des applications web ou « client léger » l'usage de deux navigateurs différents.

SENSIBILISATION DE L'UTILISATEUR

La mise en œuvre de mesures de sécurité, spécifiquement destinées à prévenir le risque d'exploitation des 0-Days, est essentielle à la protection des systèmes d'information déployés. Certaines mesures peuvent s'avérer impopulaires auprès des utilisateurs finaux.

Informer l'usager d'un SI est un élément indispensable à la prévention des 0-Days. La sensibilisation aux bonnes pratiques permettant de lutter contre les intrusions informatiques (et les 0-Days en particulier) doit faire l'objet d'un chapitre dédié dans la Charte d'utilisation des moyens informatiques de l'entreprise ou de l'administration concernée.

La Charte peut inclure une mise en garde des utilisateurs contre les vecteurs d'exploitation de 0-Days les plus fréquents (les liens html envoyés dans les courriels, la navigation sur des sites Web compromis) et décrire les bonnes pratiques à respecter.

La prévention des 0-Days passant parfois par des mesures impopulaires (listes blanches et noires des sites consultables, désactivation d'extensions ou impossibilité par l'utilisateur de modifier les options de son navigateur), cette sensibilisation doit rester pédagogique.

Par ailleurs il est recommandé que le service informatique mette en œuvre les actions suivantes :

- **Rappels réguliers des modalités internes à l'organisme de diffusion et des consignes à respecter en cas d'attaque liée à une vulnérabilité 0-Day.**
- **Mise en place d'une procédure de déclaration d'incident.**
- **Pratique d'une veille approfondie. Cette veille permet de prendre connaissance des 0-Days publiés, des contre-mesures applicables et dès que possible des correctifs associés.**
- **Sauvegardes régulières des données enregistrées sur le réseau.**

Les sauvegardes régulières ne sont pas propres au traitement des 0-Days, mais constituent une règle d'hygiène de base, propre à favoriser la continuité d'activité.

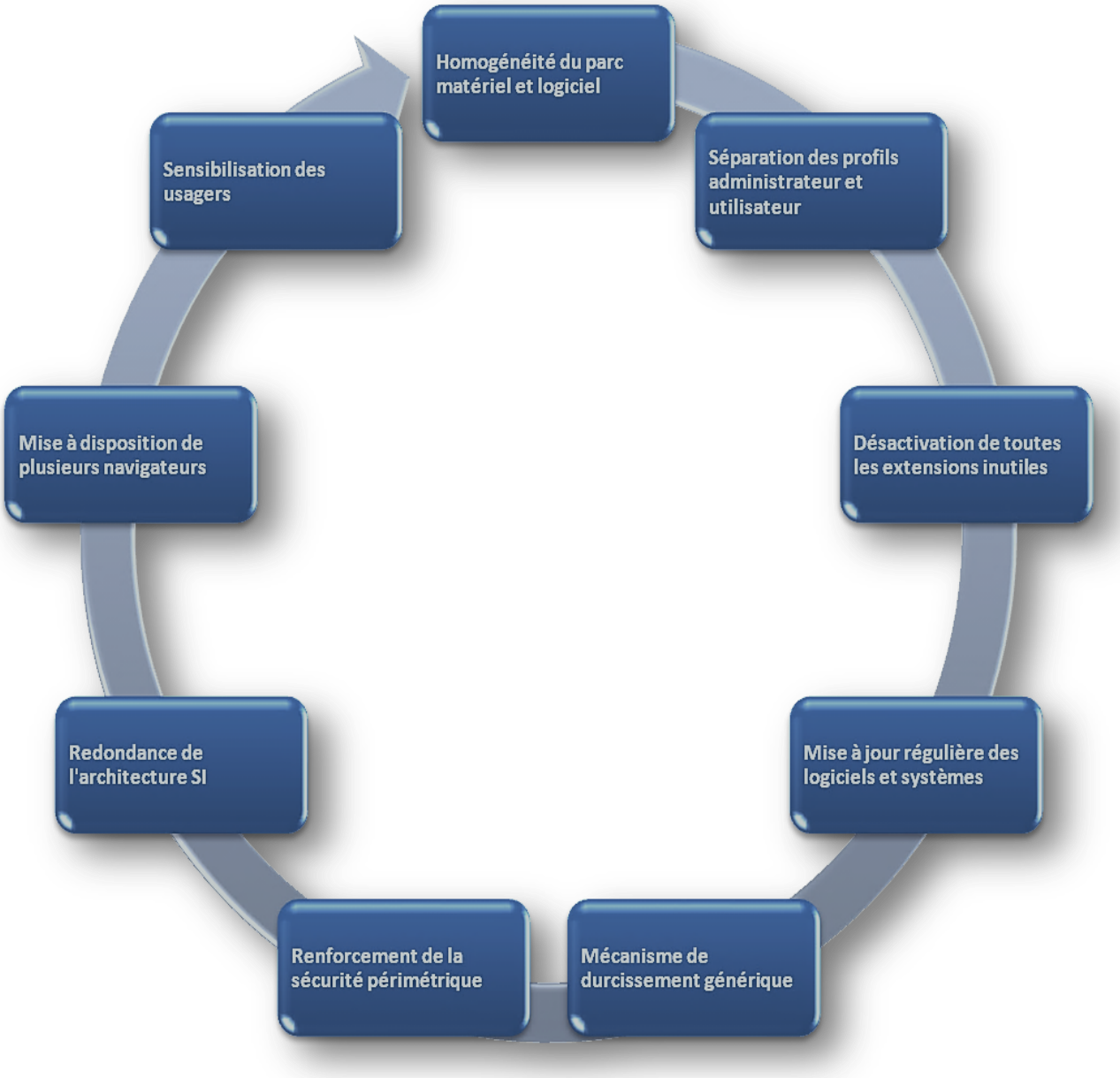
QUE FAIRE EN EN CAS D'INCIDENT

- **Il faut immédiatement déconnecter les machines du réseau, isoler la ou les machines suspectées d'avoir été infectées et alerter le ou les responsables sécurité ;**
- **Il faut alerter le CERT dont l'entreprise ou l'administration concernée dépend ;**
- **Il faut faire réaliser une copie physique du disque ;**
  - Seule la copie de bas niveau garantit l'intégralité des informations contenues sur le disque, y compris des secteurs non occupés.
- **Il faut rechercher toutes les traces disponibles (journaux des pare-feux, routeurs, outils de détection d'intrusion).**
  - Une fois les traces recueillies, il faut les copier, les dater et les signer numériquement.

Dans une seconde étape, il faut réinstaller ou faire réinstaller complètement le système d'exploitation à partir d'une version saine, puis supprimer tous les services inutiles, appliquer les correctifs de sécurité, restaurer les données d'après une copie de sauvegarde non compromise. En outre, vous changerez tous les mots de passe du système d'information.

- Lorsque ces mesures s'avèrent insuffisantes et qu'il apparaît qu'un ou plusieurs postes ont été compromis, il faut se référer à la note d'information du CERTA « Les bons réflexes en cas d'intrusion sur un système d'information ».disponible à l'adresse : http://certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

Check-List


Homogénéité du parc matériel et logiciel
Séparation des profils administrateur et utilisateur
Désactivation de toutes les extensions inutiles
Mise à jour régulière des logiciels et systèmes
Mécanisme de durcissement générique
Renforcement de la sécurité périmétrique
Redondance de l'architecture SI
Mise à disposition de plusieurs navigateurs
Sensibilisation des usagers

Agence nationale de sécurité des systèmes d'information
ANSSI – 51 boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
Sites Internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr

Contact : communication@ssi.gouv.fr

Version 1.1 – Novembre 2013
20131127-1520