RECOMMANDATIONS POUR LA PROTECTION DES SYSTÈMES D'INFORMATION ESSENTIELS

GUIDE ANSSI

ANSSI-PA-085
18/12/2020

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Informations

Attention

Ce document rédigé par l'ANSSI présente les **« Recommandations pour la protection des systèmes d'information essentiels »**. Il est téléchargeable sur le site `www.ssi.gouv.fr`.
Il constitue une production originale de l'ANSSI placée sous le régime de la « Licence Ouverte v2.0 » publiée par la mission Etalab [40].
Conformément à la Licence Ouverte v2.0, le guide peut être réutilisé librement, sous réserve de mentionner sa paternité (source et date de la dernière mise à jour). La réutilisation s'entend du droit de communiquer, diffuser, redistribuer, publier, transmettre, reproduire, copier, adapter, modifier, extraire, transformer et exploiter, y compris à des fins commerciales.
Sauf disposition réglementaire contraire, ces recommandations n'ont pas de caractère normatif ; elles 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 reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

Évolutions du document :

VERSION	DATE	NATURE DES MODIFICATIONS
1.0	18/12/2020	Version initiale

Table des matières

1
Préambule

1.1 Objectif du guide

La *directive (UE) n°2016/1148 du Parlement Européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* [1] vise à sécuriser les systèmes d'information (SI) contribuant aux activités sociétales ou économiques critiques des États membres. Cette directive est communément appelée ***directive NIS*** [1] pour *Network and Information system Security* et parfois directive SRI pour sécurité des réseaux et des systèmes d'information.

Ce guide a pour objectif d'accompagner la mise en œuvre technique des règles 7 à 16 [2] de la directive NIS sur des systèmes d'information. Ce guide s'adresse en particulier :

- aux ***opérateurs de services essentiels (OSE)***, directement soumis à la directive NIS et à la *loi n°2018-133 du 26 février 2018* [3] de transposition de la directive en droit français. Ce cadre réglementaire, détaillé au chapitre 2.1, définit des règles de sécurité applicables à certains SI dits ***systèmes d'information essentiels (SIE)***. Ce guide précise comment mettre un SIE en conformité avec ces règles de sécurité ;
- aux ***fournisseurs de services numériques (FSN)***. La directive NIS précise que les FSN ne sont pas soumis aux règles applicables aux OSE. Cependant, les FSN doivent définir eux-mêmes des « mesures de sécurité visant à assurer un niveau de sécurité des réseaux et systèmes d'information qu'ils utilisent », au titre du *règlement d'exécution (UE) 2018/151 de la commission du 30 janvier 2018* [2]. Ce guide peut servir de référence à la définition et à la mise en œuvre de ces mesures de sécurité.

Ce guide constitue également un recueil de bonnes pratiques pouvant intéresser :

- les ***opérateurs d'importance vitale (OIV)***, soumis aux articles L. 1332-6-1 et suivants du code de la défense [3], pour sécuriser les systèmes d'information d'importante vitale (SIIV) des OIV. L'annexe A du présent document propose une matrice de correspondance entre les règles de sécurité applicables aux OSE et celles applicables aux OIV ;
- toute **entité ayant des besoins de protection de ses SI** ;
- les prestataires tels que les entreprises de services numériques (ESN) concevant ou exploitant des systèmes d'information pour le compte des entités précédentes (dans les limites précisées en 2.3.3).

1. Les mots en ***gras italique*** sont définis dans le glossaire en annexe de ce guide.
2. Au sujet de la couverture des règles NIS par ce guide, voir section 2.2.
3. Ces articles ont été créés par la *loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019* dite « LPM » [7].

Au sein de ces organisations, le guide intéressera les équipes chargées de la conception et de la mise en œuvre des SI (architectes, DSI, administrateurs, etc.) ou de leur sécurité (RSSI, équipes de sécurité opérationnelle, etc.).

1.2 Contenu du document

Ce guide est organisé de la façon suivante :

- le chapitre 2 présente le cadre réglementaire associé à la transposition de la ***directive NIS*** en droit français ;
- le chapitre 3 décrit les mesures de sécurité applicables à l'architecture des SI, comme la gestion de configuration, le cloisonnement, le filtrage et la gestion des accès distants ;
- le chapitre 4 aborde la sécurité de l'administration des SI ;
- le chapitre 5 s'intéresse à la gestion des identités et des accès : identification, authentification et autorisation ;
- enfin, le chapitre 6 fait des recommandations relatives au maintien en conditions de sécurité des SI.

Information

Cette organisation suit la structure du chapitre II des règles de sécurité associées à la ***directive NIS*** définies par *l'arrêté du 14 septembre 2018* [6], et en particulier des règles 7 à 16. Ce lien structurel est détaillé dans le chapitre 2.2.

La lecture séquentielle de ce guide convient pour un opérateur de service essentiel cherchant à mettre en conformité un SIE, puisque cet objectif implique de répondre à toutes les exigences de l'arrêté et donc de prendre en compte l'ensemble des recommandations du présent guide. Cependant, l'ordonnancement des chapitres ne préjuge pas de l'ordre dans lequel une entité doit mener les chantiers de mise en conformité et de sécurisation.

Par ailleurs, un lecteur considérant ce guide comme un recueil de bonnes pratiques en matière de sécurité des SI et souhaitant l'appliquer à la conception d'un nouveau SI peut choisir un autre ordre de lecture. Il est recommandé à ce lecteur de réaliser préalablement une analyse de risque [30], pour identifier les chantiers les plus importants en fonction des enjeux métier et des menaces identifiées, puis d'adapter sa lecture en conséquence. Par exemple, si l'analyse de risque montre que les risques de latéralisation et d'élévation de privilège sont importants, le lecteur peut s'intéresser d'abord au cloisonnement et au filtrage (sections 3.2 et 3.4), au SI d'administration (chapitre 4) et à la gestion d'identité et des droits (section 5), avant de s'intéresser aux autres sections.

1.3 Convention de lecture

1.3.1 Niveaux de sécurité

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* et l'utilisation de l'icône ⚖ signifient que la recommandation est directement liée à une mesure de sécurité formulée dans la réglementation (c'est-à-dire dans une des règles de l'arrêté, section 2.1). La formulation *il est recommandé* est utilisée pour tout ce qui relève des bonnes pratiques et qui complète la réglementation.

Pour certaines recommandations de ce guide, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée complémentaire

Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée aux entités qui sont matures en sécurité des systèmes d'information.

Dans une démarche permanente de gestion du risque numérique et d'amélioration continue de la sécurité des systèmes d'information [4], la pertinence de mise en œuvre des recommandations décrites dans ce document doit être périodiquement réévaluée.

Quelles que soient les recommandations finalement retenues, l'application de ces mesures ne peut en aucun cas remplacer une évaluation du niveau de sécurité du SI par un audit, ni dispenser d'évaluer le niveau de risque résiduel sur les actifs métier (cf. 2.3.2).

La liste récapitulative des recommandations est disponible en page 99.

4. Se reporter au guide ANSSI relatif à la maîtrise du risque numérique [32].

1.3.2 Objectifs

Au début des sections principales, des encarts rappellent les objectifs visés par la réglementation.

Objectif

Description de l'objectif poursuivi par la règle associée à la section courante.

1.3.3 Scénarios d'attaque

Tout au long de ce document, des scénarios d'attaques sont présentés de la façon suivante :

Scénario d'attaque

Description d'un contexte puis de vulnérabilités et de techniques grâce auxquelles un attaquant compromet un système d'information.

Chaque scénario aide à comprendre le contexte dans lequel se fait une recommandation et les enjeux de sécurité associés.

Cependant, un scénario n'est qu'une illustration parmi d'autres d'un type d'attaque. Le lecteur ne doit donc pas chercher à contrer l'attaque présentée, mais bien à appliquer pleinement la recommandation associée.

1.3.4 Exemples

Dans le document, des exemples sont donnés pour illustrer la mise en œuvre d'une recommandation :

Exemple

Exemple de solution pour mettre en œuvre une recommandation.

Les solutions données en exemple ne constituent pas l'unique façon de traiter le problème illustré et sont obligatoirement à replacer dans leur contexte.

1.3.5 Définitions

Les termes en gras et italique, comme cet ***exemple***, sont définis dans le glossaire à l'annexe B.

D'autres définitions importantes pour la compréhension du document sont présentes à la fois dans le corps du document et dans le glossaire. Ces définitions apparaissent ainsi dans le corps du document :

Définition

Exemple de définition importante, reprise en annexe B.

2
Dispositif NIS

2.1 Cadre réglementaire

La ***directive NIS*** est une directive adoptée par l'Union européenne. À la différence d'un *règlement* communautaire qui s'applique directement et uniformément dans l'Union, une *directive* donne des objectifs à atteindre par les États membres, avec un délai de transposition. La directive NIS a donc été complétée par plusieurs textes européens et nationaux. Chaque texte national précise les secteurs et types d'opérateurs auxquels la directive s'applique dans l'État membre, ainsi que les règles de sécurité à mettre en œuvre.

La figure 2.1 reprend les différents textes applicables et leur articulation. La colonne de droite évoque, de façon simplifiée, le cadre réglementaire applicable aux opérateurs d'importance vitale et fait un parallèle avec celui de la directive NIS ; ce cadre n'est cependant pas détaillé ici.

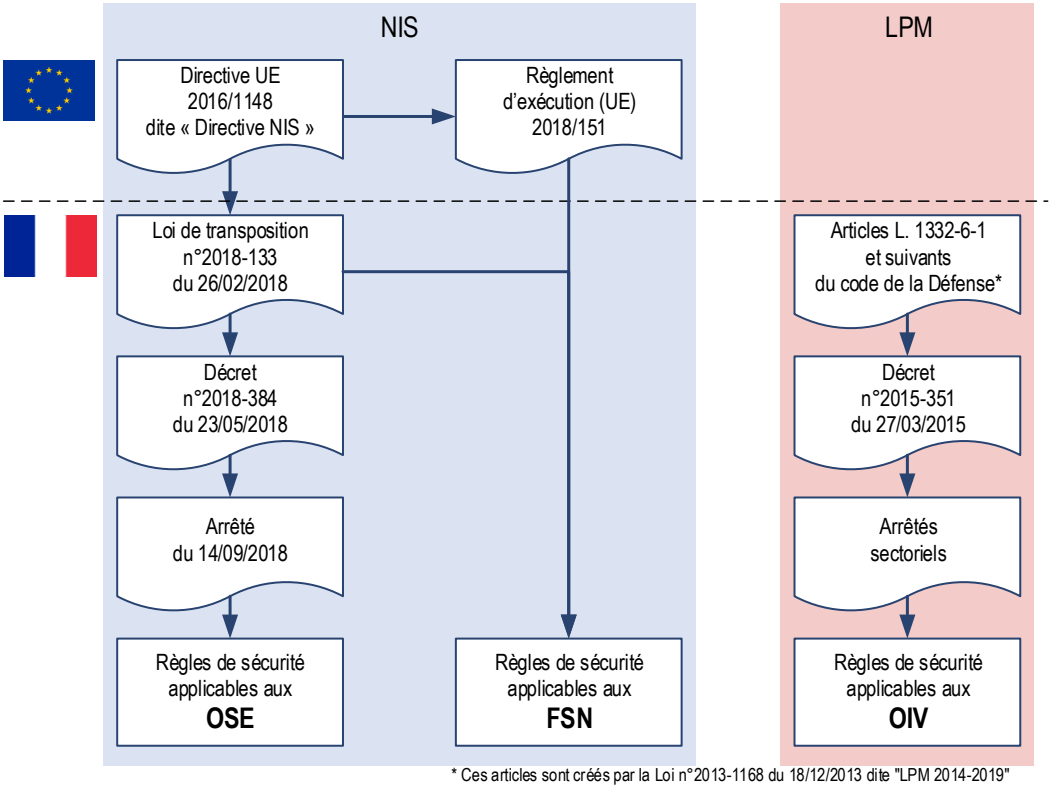

FIGURE 2.1 – Organisation du dispositif réglementaire NIS et comparaison avec celui applicable aux OIV

En France, le cadre réglementaire applicable est constitué des textes suivants.

Règlement d'exécution (UE) 2018/151 du 30 janvier 2018 [2]

Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la [directive NIS [1]] précisant les éléments à prendre en compte par les *fournisseurs de service numérique* pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information [...].
Ce règlement dispose dans son considérant n°1 que les FSN « restent libres de prendre les mesures techniques et organisationnelles qu'ils jugent appropriées et proportionnées pour gérer les risques qui menacent la sécurité de leurs réseaux et systèmes d'information, pour autant que ces mesures garantissent un niveau de sécurité approprié et tiennent compte des éléments prévus dans ladite directive ».

Loi n°2018-133 du 26 février 2018 [3]

Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Cette loi transpose dans son titre Ier la directive NIS. Cette loi dispose dans son article 6 que « le Premier ministre fixe les règles nécessaires à la protection des réseaux et systèmes d'information ».

Certaines définitions fondamentales présentées dans le glossaire de l'annexe B sont directement issues du texte de cette loi de transposition :

- ***réseau et système d'information*** (article 1) ;
- ***sécurité des réseaux et systèmes d'information*** (article 1) ;
- ***opérateurs de services essentiels*** (article 5) ;
- ***service numérique*** (article 10) ;
- ***fournisseur de service numérique*** (article 10).

Décret n°2018-384 du 23 mai 2018 [4]

Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
Concernant les OSE, l'article 10 dispose qu'un arrêté fixera les règles de sécurité et les délais d'application associés. Il s'agit de *l'arrêté du 14 septembre 2018* cité plus loin.
Concernant les FSN, l'article 18 indique que les mesures de sécurité sont prévues par le *règlement d'exécution 2018/151*.
Ce décret dresse, dans son annexe 2, la « liste des services essentiels au fonctionnement de la société ou de l'économie » répartis en secteurs, sous-secteurs et types d'opérateurs. Le décret renvoie à un arrêté pour la liste des OSE.

Arrêté du 13 juin 2018 [5]

Arrêté du 13 juin 2018 fixant les modalités des déclarations prévues aux articles 8, 11 et 20 du décret n°2018-384 [...]. Cet arrêté concerne la déclaration des réseaux et SI des OSE et la déclaration des incidents par les OSE ou les FSN.

Arrêté du 14 septembre 2018 [6]

Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n°2018-384 [...]. Cet arrêté détaille les règles de sécurité applicables aux SIE et notamment, dans son chapitre II, les règles relatives à la *protection* des réseaux et systèmes d'information, sujet de ce guide.

2.2 Couverture des règles de l'arrêté

Les règles de l'*arrêté du 14 septembre 2018* sont organisées en quatre chapitres couvrant les domaines suivants associés aux réseaux et systèmes d'information : gouvernance, protection, défense et résilience.

Ce guide se concentre sur les règles 7 à 16, c'est-à-dire celles du chapitre II, *Règles relatives à la protection des réseaux et systèmes d'information*, à l'exception de la règle 17 relative à la sécurité physique et environnementale.

Pour se mettre en conformité avec les règles des autres chapitres, le lecteur peut se reporter à d'autres documents disponibles sur le site Web de l'ANSSI [5], comme représenté sur la figure 2.2 :

- la méthode EBIOS Risk Manager [30] ;
- guide pour l'élaboration d'une politique de sécurité des systèmes d'information [17] ;
- l'homologation de sécurité en neuf étapes simples [23] ;
- élaboration des tableaux de bord de la SSI [18] ;
- cartographie du système d'information [29] ;
- prestataires d'audit de la sécurité des systèmes d'information. Référentiel d'exigences [35] ;
- prestataires de détection des incidents de sécurité. Référentiel d'exigences [36] ;
- prestataires de réponse aux incidents de sécurité. Référentiel d'exigences [37] ;
- recommandations de sécurité pour la mise en œuvre d'un système de journalisation [20].

Ce guide ne rentre pas dans le détail de l'implémentation technique des différentes solutions possibles pour protéger des systèmes d'information. Lors de la mise en œuvre des recommandations, le lecteur peut aussi se reporter aux guides détaillés cités dans la bibliographie.

5. https://www.ssi.gouv.fr

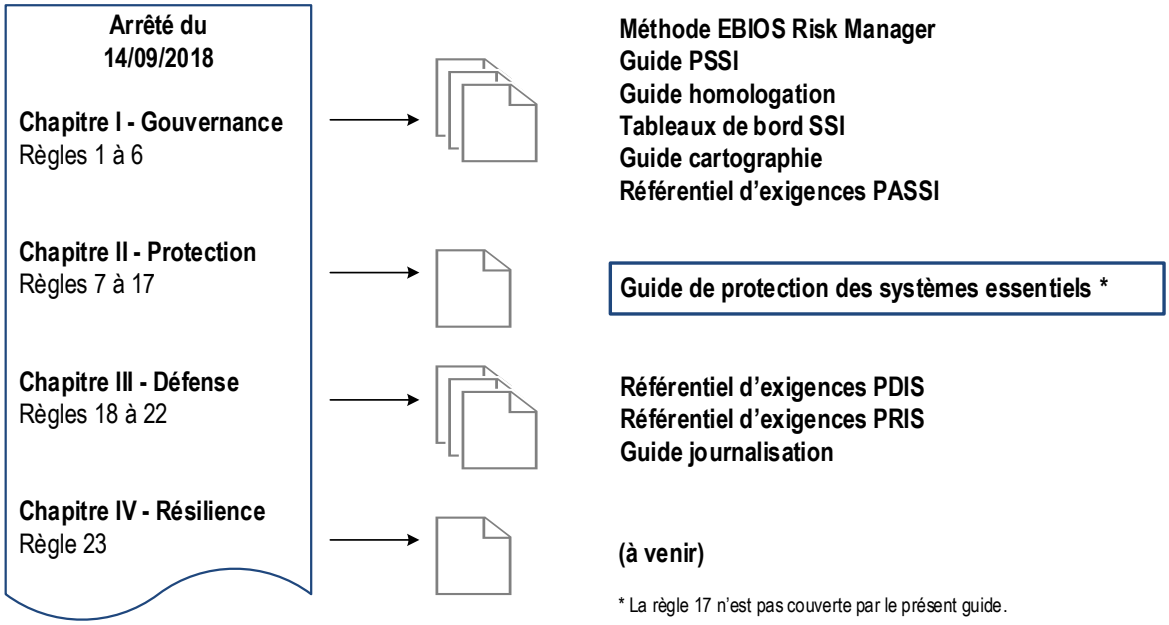

FIGURE 2.2 – Documentation applicable aux règles de sécurité

2.3 Contexte d'application des recommandations

Cette section détaille l'interprétation et l'application des recommandations de sécurité de ce guide. Elle répond aux questions suivantes :

- L'application des recommandations est-elle nécessaire ou facultative ? Comment faire si la mise en œuvre d'une recommandation est impossible ? Voir section 2.3.1.
- Comment valider la mise en conformité d'un SIE ? Voir section 2.3.2.
- Comment appliquer une recommandation sur un SI fourni ou maintenu par un prestataire ? Voir section 2.3.3.
- Sur quels produits et prestataires s'appuyer pour appliquer les recommandations ? Voir section 2.3.4.

2.3.1 Interprétation des recommandations

En fonction du public concerné, les recommandations de ce guide ont une valeur différente.

- Les ***opérateurs de services essentiels (OSE)*** ont une obligation réglementaire de mettre leurs ***systèmes d'information essentiels (SIE)*** en conformité avec les règles de sécurité énoncées dans *l'arrêté du 14 septembre 2018*. Dans ce contexte, la mise en œuvre des recommandations de ce guide est nécessaire [6] pour obtenir le niveau de sécurité visé.

6. Hors recommandations Rx+.

- Les ***fournisseurs de service numérique (FSN)*** sont soumis au *règlement d'exécution 2018/151* qui prévoit que :
  - les FSN définissent eux-mêmes des mesures techniques et organisationnelles de sécurité « pour autant que ces mesures garantissent un niveau de sécurité approprié et tiennent compte des éléments prévus dans [la directive NIS] [7] » ;
  - « les politiques sur l'architecture de la sécurité pourraient prévoir en particulier la séparation des réseaux et des systèmes ainsi que des mesures de sécurité spécifiques aux opérations critiques telles que les activités d'administration » [8].

  Les FSN pourront appliquer les recommandations de ce guide s'ils les jugent pertinentes au regard des risques pesant sur leurs SI, ou définir un autre ensemble d'exigences plus adapté à leur situation.
- ***Les opérateurs d'importance vitale (OIV)***, soumis à *loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire [...] (LPM)*, doivent répondre à des exigences très proches des règles de sécurité NIS mais définies par des arrêtés sectoriels. Appliquer les recommandations de ce guide contribue à la mise en conformité des systèmes d'information d'importance vitale à la LPM.
- Pour les autres entités, les recommandations font office de bonnes pratiques.

Dans des cas très particuliers, la mise en œuvre d'une recommandation de ce guide peut être techniquement impossible sur un SIE.

Certaines règles (9, 11, 12, 13 et 14) prévoient explicitement des conditions qui peuvent justifier, par exception, une mise en œuvre dégradée de la règle. Ainsi, un SIE, remplissant les conditions décrites dans la règle, peut être conforme à la règle même s'il ne met pas en œuvre ou s'il met en œuvre partiellement la recommandation décrite dans ce guide pour cette règle.

À l'inverse, si la règle ne prévoit pas d'exception ou si les conditions de ces exceptions ne sont pas remplies, alors l'OSE doit mettre le SIE en conformité avec la règle de sécurité et démontrer l'atteinte des objectifs de sécurité associés à cette règle, par d'autres moyens plus adaptés que l'application stricte de la recommandation de ce guide.

Dans tous les cas, l'opérateur utilise le processus d'homologation pour réévaluer les risques résiduels découlant de cette situation dégradée ou atypique, et pour décrire les mesures compensatoires finalement mises en œuvre dans le dossier d'homologation du SIE.

2.3.2 Processus d'homologation

La règle 3 « homologation de sécurité » de *l'arrêté du 14 septembre 2018* décrit la procédure qu'un OSE doit suivre pour attester « que les risques pesant sur la sécurité de ce système ont été identifiés et que les mesures nécessaires pour le protéger sont mises en œuvre. Elle atteste également que les éventuels risques résiduels ont été identifiés et acceptés par l'opérateur ». L'opérateur peut se reporter au guide ANSSI de l'homologation de sécurité en neuf étapes simples [23].

7. Voir le considérant n°1 du règlement d'exécution [2].
8. Voir le considérant n°6 du règlement d'exécution [2].

Attention

L'application des mesures présentées dans ce guide ne peut en aucun cas remplacer une évaluation du niveau de sécurité du SI et la validation de sa conformité à la ***directive NIS***. Ces constats formels ne peuvent être validés que par un audit réalisé dans les conditions fixées par la règle 5 « audits de sécurité ».
Ces constats sont également versés au dossier d'homologation et examinés par l'autorité d'homologation.

Il est fortement recommandé aux autres opérateurs, dont les FSN, de recourir également à l'homologation pour formaliser les risques encourus et ceux effectivement couverts.

2.3.3 Opérateurs et prestataires

La mise en conformité d'un SI à la réglementation est de la responsabilité de l'opérateur. L'opérateur peut choisir de garder la charge de l'implémentation pratique des mesures de sécurité ou de transférer contractuellement cette charge à un prestataire.

Lorsque l'opérateur confie tout ou partie de la conception ou de l'exploitation d'un SIE à un prestataire, le contrat doit prévoir les mesures de sécurité que le prestataire doit mettre en œuvre [9]. L'opérateur doit vérifier la mise en œuvre effective de ces mesures par le prestataire.

L'opérateur ne peut donc dégager sa responsabilité en confiant tout ou partie d'un SIE à un prestataire. Le niveau de sécurité exigé pour un SIE est le même, que celui-ci soit directement géré par l'opérateur ou qu'il soit confié à un prestataire. Dans tous les cas, l'opérateur reste seul responsable du respect des règles de sécurité.

Par convention, ce guide emploie le terme *opérateur* pour désigner l'entité qui met en œuvre les recommandations, que ce soit l'opérateur ou un prestataire qu'il aura mandaté à cet effet.

2.3.4 Utilisation de produits et services de confiance

Tout au long de ce guide, il est recommandé aux opérateurs de mettre en œuvre des mesures de sécurité afin de protéger leurs SIE. L'opérateur est responsable de l'efficacité de ces mesures. Un moyen de garantir cette efficacité consiste à choisir des produits et des services de sécurité disposant d'un visa de sécurité de l'ANSSI.

Si l'opérateur met en œuvre un produit de sécurité ayant obtenu un visa de sécurité [10] de l'ANSSI, ce produit est considéré comme étant *de confiance*, dans les conditions précisées par le visa. Plus le niveau d'assurance recherché par la certification ou la qualification associée au visa est élevé, plus le produit a été évalué dans le détail, et plus la confiance est élevée. Il est donc fortement recommandé de privilégier des produits ayant obtenu un visa de sécurité ANSSI – et en particulier ceux ayant obtenu une qualification – lorsqu'ils existent.

9. Le lecteur peut à ce sujet consulter le guide *Maîtriser les risques de l'infogérance – Externalisation des systèmes d'information* [14] de l'ANSSI.

10. L'opérateur peut se référer au site Web de l'ANSSI pour connaître les différents visas de sécurité, avoir la liste des prestataires et produits ayant reçu un visa de sécurité, le type du visa correspondant et les fonctionnalités vérifiées : `https://www.ssi.gouv.fr/visa-de-securite`.

Si l'opérateur déploie un produit n'ayant pas de visa de sécurité, alors il a la responsabilité de vérifier que le produit fournit effectivement les fonctions de sécurité attendues.

Cette approche est la même pour les prestations de services. Un prestataire qualifié fournissant une prestation qualifiée est considéré comme étant ***de confiance*** par défaut, alors que si la prestation n'est pas qualifiée, l'opérateur a la responsabilité de s'assurer du respect des exigences de sécurité par son prestataire.

3
Sécurité de l'architecture (règles 7 à 10)

Ce chapitre détaille les recommandations relatives à la section 1 du chapitre II de l'*arrêté du 14 septembre 2018*. Il couvre les règles relatives à la configuration lors de l'installation de services et d'équipements (règle 7), au cloisonnement des SIE (règle 8), aux accès distants aux SIE (règle 9) et au filtrage des flux de données circulant dans les SIE (règle 10).

3.1 Configuration (règle 7)

Objectif

Limiter les éléments techniques du SIE qui peuvent être utilisés pour réaliser une attaque, en installant sur le SIE uniquement les services et équipements indispensables, et en gérant en particulier les supports amovibles.

Dans le contexte de la règle 7, le renforcement du niveau de sécurité du SIE passe par un durcissement (*hardening*) incluant :

- la limitation et une configuration adaptée des fonctions présentes sur le SIE (section 3.1.1) ;
- la maîtrise des éléments matériels du SIE (section 3.1.2) ;
- la gestion des supports amovibles, vecteurs d'ingestion de données vers le SIE (section 3.1.3).

3.1.1 Réduction de la surface d'attaque

Surface d'attaque

L'ensemble des éléments techniques du SI qui peuvent être utilisés pour réaliser une attaque. Une ***surface d'attaque*** est d'autant plus large que le nombre d'éléments distincts est grand ou que ces derniers présentent des ***vulnérabilités*** exploitables par un attaquant.

Un concept lié à la surface d'attaque est celui de vecteur d'attaque. Les vecteurs d'attaque sont les aspects d'un système qui peuvent être utilisés ou détournés pour réaliser une attaque sur ce système. Dans le contexte d'un système d'information, les vecteurs d'attaque peuvent être des éléments techniques, mais aussi humains ou organisationnels. Les vecteurs d'attaque *techniques* composent donc la surface d'attaque d'un SI.

3.1.1.1 Modification de la configuration par défaut

Pour faciliter ou accélérer leur installation, les composants matériels ou logiciels peuvent être installés dans le SIE selon une configuration par défaut établie par leur éditeur ou leur fabricant. La configuration obtenue est alors identique d'une installation à une autre. Des informations relatives à cette configuration sont alors souvent facilement accessibles, en source ouverte. Parfois, la configuration ne respecte pas le principe de moindre privilège. Dans les deux cas, cette pratique augmente la surface d'attaque.

La configuration d'un composant inclut par exemple :

- les comptes techniques et éléments d'authentification associés, comme les identifiants et mots de passe (notamment les combinaisons dites « triviales », comme `admin/admin` ou `root/root`) ;
- les ports réseau utilisés ;
- les répertoires d'installation et de travail ;
- les droits d'accès sur les répertoires et fichiers (notamment des droits d'accès permissifs pour faciliter l'installation, mais qui ne sont pas modifiés lors de la finalisation du processus d'installation) ;
- le compte utilisé pour exécuter un service ou un processus, et les droits associés à ce compte (attribution de privilèges plus élevés que nécessaire) ;
- les fichiers de configuration des éléments de sécurité, en particulier de traçabilité.

Scénario d'attaque

Un service d'un SIE est installé dans sa configuration par défaut, sans que les éléments d'authentification du compte administrateur soient modifiés.
Un attaquant identifie le type du service et se documente sur les éléments d'authentification par défaut. Il prend ensuite facilement le contrôle du service.

L'exploitation par un attaquant des configurations par défaut est facilitée par des outils automatisant l'inventaire de SI et de leurs vulnérabilités, puis l'exploitation des vulnérabilités découvertes. On peut citer à titre d'exemple ces types d'outils :

- des outils de découverte (*scan*) du réseau qui permettent d'obtenir la liste des systèmes et les services exécutés sur chacun de ces systèmes. Un attaquant obtient ainsi la liste des services présents dans un SI, qu'ils soient utilisés ou non ;
- des outils d'inventaire des vulnérabilités. Un attaquant obtient ainsi une liste de vulnérabilités présentes sur un système et pouvant potentiellement être exploitées ;
- des outils d'exploitation de vulnérabilités, qui permettent notamment d'exécuter sur un système des programmes spécialisés exploitant une vulnérabilité connue. Un attaquant obtient ainsi le plus souvent un accès privilégié au système attaqué.

R1

⚖ Modifier les éléments de configuration par défaut

Lors de l'installation ou de la réinstallation des services et équipements du SIE, il est fortement recommandé que l'opérateur modifie les éléments de configuration fixés par défaut dès lors qu'ils sont exploitables par un attaquant.
En particulier, l'opérateur doit modifier les éléments secrets d'authentification pour les comptes techniques ou les comptes d'administration (section 5.2.1).

Information

Certaines modifications dans la configuration ou dans l'intégration d'un produit remettent en question son fonctionnement, sa sécurité ou sa garantie. Il est donc pertinent de travailler avec le fournisseur du produit pour définir les réponses aux exigences de sécurité.

Concernant les paramètres d'installation par défaut (répertoires, droits d'accès, etc.), l'opérateur doit s'interroger sur leur sécurité par rapport à ses besoins. Si ces paramètres par défaut créent une vulnérabilité, alors l'opérateur doit les modifier pour réduire la surface d'attaque ; sinon, il peut les conserver.

Par exemple, les ports réseau utilisés par un service sont souvent standardisés. Bien que ces ports soient facilement identifiables par un attaquant, ils ne constituent pas une vulnérabilité. De plus, les changer peut créer des difficultés d'intégration, d'interopérabilité, voire de maintenance de la solution. Les ports par défaut peuvent donc en général être conservés.

À l'inverse, les bannières applicatives configurées par défaut et renvoyées par les services numériques facilitent les opérations de ciblage d'un attaquant. Ces bannières représentent donc une menace et doivent être supprimées.

Concernant les éléments d'authentification, l'opérateur doit se documenter sur les comptes créés par défaut, les secrets d'authentification et les droits associés à ces comptes. Au besoin, il peut interroger le fournisseur pour s'assurer qu'il a bien traité tous les comptes concernés, notamment ceux dont les éléments d'authentification ou les droits ne peuvent pas être changés.

Enfin, si le service crée un compte privilégié, et notamment un compte d'administrateur de domaine dans un environnement Windows, l'opérateur doit également interroger le fournisseur pour identifier les privilèges effectivement nécessaires, puis les ajuster dans l'annuaire.

R1 -

Pallier l'impossibilité de changer un élément par défaut

Lorsque des raisons techniques empêchent de modifier un élément de configuration par défaut, et en particulier des éléments d'authentification ou des droits trop étendus, il est fortement recommandé que l'opérateur mette en œuvre des mesures techniques ou organisationnelles pour réduire les risques associés à ces éléments par défaut.
Il est recommandé que l'opérateur décrive les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.

Parmi les mesures techniques possibles pour réduire le risque d'une action malveillante, l'opérateur peut limiter la surface d'attaque par du cloisonnement (emploi de conteneurs ou isolation dans une DMZ, voir section 3.2) et du filtrage (filtrage local des accès au niveau de la ressource, voir section 3.4). L'opérateur peut également renforcer la journalisation et la supervision des accès à la ressource.

3.1.1.2 Restriction des fonctionnalités accessibles

Les services et les équipements peuvent parfois être installés sous forme de modules, obligatoires ou facultatifs. Parmi ces modules, seuls certains sont utiles au fonctionnement ou à la sécurité du SIE et font donc l'objet d'une configuration appropriée, d'une maintenance régulière et d'une supervision. Par facilité ou par négligence, d'autres modules dont le SIE n'a pas l'usage peuvent rester actifs et être accessibles aux attaquants, alors qu'ils ne sont pas configurés, maintenus ou supervisés avec le même soin.

Scénario d'attaque

Un serveur Web est actif au sein d'un SIE, mais il n'est plus utilisé. Comme il n'est plus indispensable, ce serveur n'est pas tenu à jour.
Un attaquant utilise un outil de découverte du réseau pour faire la liste des services en écoute et de leurs niveaux de sécurité. Il détecte ainsi le serveur Web obsolète et en prend facilement le contrôle.
L'attaquant peut alors rebondir vers son objectif principal au sein du SIE.

R2

⚖ Installer uniquement les services ou fonctionnalités indispensables

L'opérateur doit installer les seuls services et fonctionnalités indispensables au fonctionnement ou à la sécurité du SIE, afin de limiter la surface d'attaque exploitable par un attaquant.
Si des services ou fonctionnalités non indispensables sont installés par défaut, l'opérateur les désinstalle.

L'opérateur doit analyser le fonctionnement technique du SIE pour exclure les services ou fonctionnalités installés mais non utilisés (modules installés, outils de développement, services en écoute sur une machine, etc.). Il peut à cet effet utiliser des outils d'audit technique ou de découverte automatique.

Si, après analyse, la désinstallation d'un service ou d'une fonctionnalité n'est pas possible, l'opérateur doit se rapprocher de l'éditeur ou du fabricant afin de prendre des mesures de réduction du risque, comme le blocage ou la supervision des accès au service, ainsi que l'inclusion du service dans le périmètre de maintien en conditions de sécurité du SIE.

R2 -

⚖ Pallier l'impossibilité de désinstaller un service non indispensable

Lorsqu'il n'est pas possible de désinstaller les services et fonctionnalités qui ne sont pas utilisés sur le SIE, l'opérateur doit désactiver ces services et fonctionnalités ou empêcher leur accès.

L'opérateur doit verser au dossier d'homologation la liste des services et fonctionnalités inutiles qu'il n'a pas été possible de désinstaller. Les raisons et les mesures de réduction de risque sont également précisées dans le dossier d'homologation.

Chaque configuration matérielle ou logicielle doit être inventoriée, par exemple sous la forme d'une configuration de référence. L'emploi de configurations de référence réduit les délais de réaction lors d'un incident de sécurité pour recouvrer une capacité de traitement.

Afin de ne pas dégrader le niveau de sécurité du SIE au fil du temps, les configurations de référence doivent être régulièrement réévaluées et mises à jour si besoin. Le maintien dans le temps de ces configurations de référence doit prendre en considération l'évolution des besoins, des fonctions disponibles sur les éléments du SI et des nouvelles menaces connues.

R3

Définir et utiliser des configurations de référence

Il est recommandé que l'opérateur définisse une ou plusieurs configurations de référence sécurisées, expurgées de tous les éléments inutiles et qu'il les utilise lorsqu'il installe un nouvel élément du SIE.
Il est recommandé que l'opérateur maintienne ces configurations de référence à jour dans la durée.
Il est recommandé que les écarts entre les configurations en production et les configurations de référence fassent l'objet d'un suivi régulier, afin de les identifier au plus tôt.

3.1.2 Maîtrise des éléments du SIE

Le maintien du niveau de sécurité du SIE dans le temps passe notamment par :

- une connaissance de l'environnement du SIE et de ce qui s'y connecte ;
- un usage d'éléments ***maîtrisés*** au sein du SIE ou pour s'y connecter.

SI maîtrisé

SI dont les éléments constitutifs sont connus, configurés et maintenus par l'opérateur ou par un de ses prestataires, et permettent de garantir le niveau de sécurité du SI.

3.1.2.1 Inventaire des éléments connectés au SIE

Afin de s'assurer que sa politique de sécurité suscite bien les effets attendus, l'opérateur doit préalablement connaître le périmètre d'application de cette politique, c'est-à-dire les éléments qui constituent le SIE. C'est en particulier l'objet de la règle 6 sur la cartographie, ainsi que d'un guide de l'ANSSI [29].

Ce périmètre doit prendre en compte les équipements pouvant se connecter au SIE [11], de façon permanente ou temporaire : poste de travail, serveur, périphérique, etc. En effet, tout élément

11. Le cas des utilisateurs qui se connectent au SIE à travers un réseau public et qui n'appartiennent ni à l'opérateur ni à l'un de ses prestataires est exclu, cf. sections 3.3 et 3.2.6.

connecté dont le niveau de sécurité est inférieur aux standards de sécurité appliqués sur le SIE abaisse le niveau de sécurité de l'ensemble du SIE.

Scénario d'attaque

Les utilisateurs se connectent au SIE depuis des postes locaux maîtrisés et dédiés au SIE. Le niveau de confiance dans les postes est donc élevé. Cependant, en cas de maintenance applicative, un prestataire peut accéder temporairement au SIE depuis ses propres locaux et ses propres postes.
L'accès étant temporaire et réalisé depuis un SI externe, il a été oublié dans la cartographie du SIE et dans l'analyse de risque réalisées par l'opérateur.
Un attaquant compromet le poste de travail du prestataire, et dispose ainsi d'un accès potentiellement non supervisé au SIE.

R4

Établir un inventaire technique des éléments et des accès au SIE

Il est fortement recommandé que l'opérateur établisse un inventaire technique des éléments composant le SIE et des éléments qui peuvent y être connectés (postes de travail, équipements, matériels périphériques, supports amovibles, etc.), physiquement ou à distance.
Dans le cas où une tierce partie se connecte au SIE, il est recommandé que l'opérateur le note dans sa cartographie et en tienne compte dans l'analyse de risque.

3.1.2.2 Utilisation d'éléments maîtrisés dans le SI

Pour connaître le niveau de sécurité des éléments de son SI, l'opérateur doit gérer ces éléments, directement ou indirectement à travers une prestation encadrée par un contrat. Cette gestion inclut couramment :

- le durcissement des systèmes et applications ;
- le déploiement de mises à jour ;
- l'administration des éléments du SI ;
- la configuration à distance des flottes d'équipements mobiles ;
- etc.

Scénario d'attaque

L'opérateur d'un SIE fournit des postes de travail à ses utilisateurs et les maintient à jour. Cependant, en cas d'astreinte, ces mêmes utilisateurs peuvent se connecter au SIE depuis leur domicile, avec leur ordinateur personnel.
Un attaquant envoie un courriel piégé à un des utilisateurs sur son adresse personnelle, et prend le contrôle de l'ordinateur personnel. Il y trouve les informations de connexion au SIE et peut à son tour accéder au SIE, à l'insu de l'utilisateur.

Afin de limiter la surface d'attaque du SIE, l'opérateur doit maîtriser les éléments qui constituent le SIE ou qui sont en interaction avec lui.

R5

⚖ Utiliser uniquement des équipements maîtrisés

L'opérateur doit s'assurer que seuls des équipements *maîtrisés* et indispensables au fonctionnement ou à la sécurité du SIE sont utilisés sur le SIE. Cela inclut les postes de travail, serveurs, équipements réseau, périphériques amovibles, etc. L'opérateur doit interdire l'utilisation de tout autre équipement.
Cette politique doit couvrir les activités des salariés internes comme celles des prestataires, que les connexions au SIE soient locales ou distantes.

En particulier, un ***SI maîtrisé*** ne peut donc intégrer les pratiques de ***bring your own device (BYOD)*** [12], où des personnes peuvent connecter au SI des équipements personnels dont l'opérateur ne maîtrise pas le niveau de sécurité [13].

Information

La maîtrise des équipements par l'opérateur (ou par le prestataire qu'il a mandaté à cet effet) doit être obtenue pour les accès des utilisateurs et des administrateurs au SIE, que ce soit ceux de l'opérateur ou de ses infogérants réguliers. Mais cette maîtrise peut être complexe à mettre en œuvre dans le cas d'intervenants occasionnels, comme des experts auxquels on fait appel pour du support de niveau 3 ou 4.

Pour ces accès ponctuels, le *référentiel d'exigences pour les prestataires d'administration et de maintenance sécurisées (PAMS)* [38] propose le concept d'*enclave d'administration tierce*, servant de tampon entre les postes moins maîtrisés des intervenants et le SIE. Le lecteur peut se reporter à la section correspondante du référentiel d'exigences.

3.1.3 Gestion des supports amovibles

Une bonne pratique consiste à distinguer les supports amovibles par usage. Ainsi, il est raisonnable de dédier des supports amovibles à des usages relatifs au SIE (section 3.1.3.1) et à prendre des précautions complémentaires lors des échanges de données entre le SIE et d'autres SI (section 3.1.3.2). Dans tous les cas, il est recommandé de surveiller les échanges réalisés au moyens de supports amovibles (section 3.1.3.3).

3.1.3.1 Dédier des supports amovibles au SIE

Scénario d'attaque

Un utilisateur possède une clé USB et la connecte suivant les cas à son poste de travail bureautique ayant accès à Internet et au SIE.
Un attaquant compromet le poste de travail grâce à un courriel piégé. L'attaquant copie un code malveillant sur la clé USB lorsqu'elle est connectée au poste de tra-

12. En français, *apportez votre équipement personnel de communication* ou AVEC.
13. Cette exclusion ne couvre pas le cas où des utilisateurs externes se connectent au SIE à travers un réseau lui aussi non maîtrisé ; ce dernier cas constitue un *accès public* et fait l'objet d'exigences particulières décrites à la section 3.3.1.

vail. Ce code est transporté *via* le support amovible et exécuté sur le SIE à l'insu de l'utilisateur.
L'attaquant peut alors modifier le SIE et continuer son attaque.

R6

⚖ Dédier aux SIE des supports amovibles identifiés

Les supports amovibles étant des vecteurs d'attaque, l'opérateur doit dédier des supports amovibles au fonctionnement des SIE (exploitation, maintenance, administration, sécurité, etc.).
Seuls ces supports peuvent être connectés au SIE. Ils ne peuvent être connectés qu'au SIE et aux systèmes explicitement prévus par l'opérateur.
Ces supports doivent être inventoriés et physiquement identifiés.

L'opérateur peut mettre en œuvre des mesures techniques ou organisationnelles permettant de contrôler l'application de cette règle, comme :

- boucher physiquement les ports USB ;
- désactiver les ports USB sur les équipements du SIE (par configuration du BIOS ou du système d'exploitation), la connexion de supports amovibles pouvant être finalement autorisée sur un petit nombre d'équipements après une validation organisationnelle ;
- utiliser des logiciels de restriction de l'utilisation des clés USB (suivant une marque ou un modèle particulier, la présence d'une signature, etc.) sur les équipements du SIE ;
- mettre en œuvre une traçabilité, organisationnelle ou technique, de l'utilisation des supports ;
- s'assurer de la protection physique des supports en les mettant dans un coffre fermé ;
- appliquer un marquage visuel clair sur les supports concernés afin de les identifier facilement.

Exemple

Un opérateur, dans une infrastructure Windows, souhaite éviter l'injection de code malveillant ou l'exfiltration de données au moyen de clés USB.
Il peut désactiver logiquement les ports USB au travers d'une stratégie de groupe (GPO). Il peut aussi désactiver ces mêmes ports au niveau du BIOS, ou boucher physiquement les ports USB.

3.1.3.2 Innocuité des supports amovibles à usage mixte

Si une passerelle d'échange (interconnexion directe) ne peut pas être mise en place, alors un support de stockage amovible peut servir à transférer de l'information entre un SIE et un autre SI. Par exemple, un SIE dépourvu d'interconnexion reçoit des mises à jour sur un support amovible.

Si la maîtrise des supports amovibles recommandée par R6 est nécessaire, elle doit être complétée par une vérification de l'innocuité du contenu des supports. Pour cela, il est nécessaire de les analyser systématiquement avant leur utilisation.

R7

⚖ Décontaminer les supports amovibles avant leur utilisation

L'opérateur doit procéder à l'analyse systématique du contenu de chaque support amovible dès sa connexion au SIE, avant de pouvoir l'utiliser.
Pour permettre cette analyse avant utilisation, il est fortement recommandé de désactiver l'exécution automatique des contenus (*autorun*).
L'analyse doit au minimum rechercher des codes malveillants par rapport à une base de connaissance à jour.

Cette recommandation est généralisée à l'ensemble des utilisations de supports amovibles, et pas seulement aux échanges d'informations avec d'autres SI.

Cette recommandation peut efficacement être complétée par d'autres mesures de lutte contre les codes malveillants : analyse du comportement de la machine, limitation des codes exécutables à une ***liste d'autorisation*** (ou liste blanche) avec utilisation possible de signatures cryptographiques pour valider l'intégrité et l'authenticité de ces codes exécutables, etc.

La recommandation R7 évoque un contrôle fait directement sur le SIE. Dans ce cas, si le contrôle est faillible, le SIE peut être compromis avant même d'avoir détecté le code malveillant. Il est possible de renforcer la défense en profondeur en déplaçant l'analyse du support amovible avant son intégration dans le SIE.

R7 +

Utiliser un équipement dédié à l'analyse des supports amovibles

Afin de limiter l'impact de l'exécution d'un code malveillant présent sur un support amovible, il est fortement recommandé d'utiliser des équipements spécifiques pour analyser les supports amovibles *avant* leur connexion au SIE.

L'opérateur peut par exemple utiliser des solutions de type ***station blanche*** ou ***sas***, dans lesquelles le support est analysé par une machine dédiée. Ces solutions peuvent intégrer les fonctions suivantes :

- analyse antivirale à partir d'une base de connaissance ;
- analyse comportementale par ouverture du document ou du code exécutable à analyser dans un environnement dédié ou ***bac à sable*** ;
- transformation des documents, depuis un format de bureautique (texte, tableau, etc.) vers un format image, afin d'éviter qu'un éventuel code intégré puisse être exécuté (***statification***) ;
- limitation des formats de fichier autorisés et validation de la structure des fichiers par rapport à des formats de référence ;
- protection des équipements contre les attaques en surcharge électrique (dites ***USB killer***) ;
- protection des équipements contre les attaques par usurpation USB (dites ***Bad USB***).

Les figures 3.1 et 3.2 illustrent le fonctionnement d'une ***station blanche*** et d'un ***sas***.

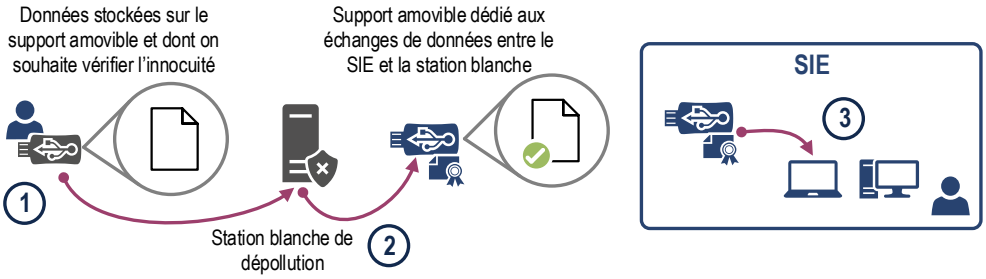

FIGURE 3.1 – Station blanche

① L'utilisateur connecte le support amovible à analyser à la station blanche et sélectionne les fichiers qu'il souhaite transférer sur le SIE.

② La station blanche analyse les fichiers et copie les fichiers sains sur un support amovible maîtrisé et dédié à l'importation et à l'exportation de données entre le SIE et la station blanche. De manière à limiter l'impact en cas de compromission de la station blanche, les transferts de données entre les deux supports de données sont réalisés en minimisant autant que possible les données temporaires. Si ces données temporaires sont inévitables, un mécanisme automatique les supprime périodiquement (ex. : quotidiennement).

③ L'utilisateur, authentifié sur le SIE, connecte le support amovible maîtrisé sur un point d'insertion de données, lequel vérifie qu'il s'agit d'un support maîtrisé et que l'analyse de sécurité a bien été faite par la station blanche. Cette action d'importation de données est journalisée et imputée à l'utilisateur.

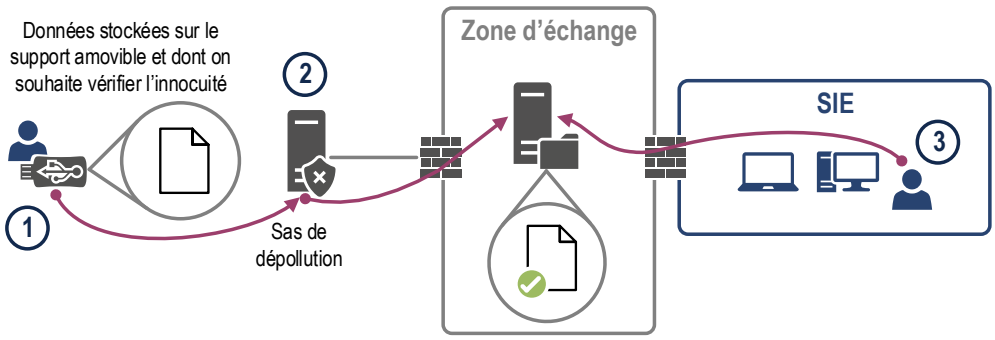

FIGURE 3.2 – Sas

① L'utilisateur connecte le support de données à analyser sur le sas et sélectionne les fichiers qu'il souhaite transférer sur le SIE.

② Le sas de dépollution analyse les fichiers et copie les fichiers sains dans la zone d'échange, dans un espace accessible uniquement de l'utilisateur ayant initié le transfert.

③ L'utilisateur, authentifié sur le SIE, télécharge les fichiers depuis la zone d'échange. Cette action d'importation de données est journalisée et imputée à l'utilisateur. De manière à limiter l'impact en cas de compromission du sas, un mécanisme automatique supprime les données de la zone d'échange. Cette suppression est faite préférentiellement à l'issue de l'importation des données sur le SIE ou, à défaut, périodiquement (ex : quotidiennement).

3.1.3.3 Traçabilité de l'utilisation des supports amovibles sur le SIE

En complément des mesures précédentes visant à maîtriser les supports amovibles et à en vérifier l'innocuité, il est recommandé que l'opérateur s'assure de la traçabilité et de l'imputabilité des connexions de supports amovibles au SIE, ainsi que des importations et exportations de données. Cela contribue à la détection des incidents de sécurité à travers la journalisation (règle 19).

R8

Mettre en œuvre une traçabilité de l'utilisation des supports amovibles

Lorsque le fonctionnement du SIE requiert l'utilisation de supports amovibles, il est fortement recommandé que l'opérateur mette en place un outil de traçabilité lui permettant d'avoir des informations sur les connexions de supports amovibles au SIE, et sur les données importées ou exportées du SIE.

R8 +

Mettre en œuvre un outil de protection contre l'exfiltration de données

Il est fortement recommandé que l'opérateur utilise un outil filtrant ce qui est extrait du SIE.

L'outil recommandé par la recommandation R8+ peut inclure les fonctions suivantes :

- limiter les formats de fichiers ou les quantités de données autorisés à être extraits du SIE ;
- inspecter les fichiers destinés à être extraits du SIE, pour détecter un éventuel marquage (données ou méta-données sensibles) dans les documents ;
- alerter l'administrateur lorsqu'une des fonctions précédentes génère une alerte.

Plus généralement, les données extraites légitimement du SIE peuvent être chiffrées pour en protéger la confidentialité.

3.2 Cloisonnement (règle 8)

Objectif

Prévenir la compromission du SIE ou contenir la propagation d'une attaque réussie en prenant des mesures de cloisonnement.

Cloisonnement

Fonction de sécurité assurant une séparation entre les éléments d'un SI sans impact sur le service rendu. Elle se met en œuvre techniquement par une ***segmentation*** du système en ***sous-systèmes***. Cette démarche restreint chaque partie du SI aux actions dont elle a besoin.

Le cloisonnement exigé par la règle 8 a pour objectifs de :

- limiter la surface d'attaque du SIE ;
- contenir – ou à défaut de ralentir – un éventuel attaquant en l'empêchant d'accéder à des éléments du SIE, aussi bien depuis l'extérieur du SIE (intrusion) que depuis l'intérieur (***déplacement latéral***) ;
- limiter l'impact d'une compromission sur le SIE en réduisant la recherche d'indicateurs de compromission à un sous-ensemble du SIE et en ayant potentiellement moins de systèmes à reconstruire ;
- permettre d'adapter finement le niveau de sécurité et les mesures à mettre en oeuvre pour chaque sous-système du SIE.

Scénario d'attaque

Un opérateur possède un site Web institutionnel et un SIE, non exposé sur Internet. Ces deux SI partagent la même infrastructure serveur virtualisée. L'opérateur ne considère pas son site Web comme critique et y applique rarement les mises à jour de sécurité, alors que ce système est très exposé.
Un attaquant prend facilement le contrôle du site Web. Il peut ensuite utiliser une vulnérabilité de l'hyperviseur, commun au site Web et au SIE, pour compromettre le SIE.

Pour répondre à l'exigence de cloisonnement, l'opérateur définit d'abord une ***segmentation*** de son SI en distinguant des groupes d'éléments suivant leurs fonctions et leurs besoins de sécurité, puis il réfléchit au ***besoin de fonctionnement*** justifiant des communications légitimes entre ces groupes (section 3.2.1). Après avoir choisi les types de cloisonnement les plus pertinents (section 3.2.2), l'opérateur met en œuvre techniquement le cloisonnement entre les différentes zones (section 3.2.3). Trois cas particuliers seront abordés pour compléter cette approche :

- le cas des SIE externalisés, dont l'architecture n'est pas directement maîtrisée par l'opérateur (section 3.2.4) ;

- le cas des SIE des infrastructures numériques qui concourent au fonctionnement d'Internet et qui y sont donc naturellement connectées (section 3.2.5) ;
- le cas des SIE ouverts au public, qui utilisent aussi un réseau non maîtrisé comme Internet et des postes d'accès dont l'opérateur ne maîtrise pas le niveau de sécurité (section 3.2.6).

Le cloisonnement s'applique à deux niveaux : segmentation des moyens physiques (réseaux, serveurs, stockage) et séparation des moyens logiques (traitements de données, flux réseau). Quand il est appliqué aux flux réseau, le cloisonnement permet la mise en œuvre du ***filtrage*** des flux entre les différents segments (section 3.4). Les concepts de cloisonnement et de filtrage sont donc distincts mais complémentaires. Par ailleurs, le concept de système isolé doit tenir compte de toutes les dimensions du cloisonnement. Deux systèmes ne sont vraiment isolés l'un de l'autre que lorsqu'ils n'ont aucun moyen physique (réseau, serveur, stockage) et logique (traitement de données et flux réseau) en commun.

3.2.1 Segmentation du SI en zones

Cette section s'intéresse à la démarche de segmentation du SI en sous-systèmes, et en particulier aux critères qui vont conduire à distinguer les sous-systèmes les uns des autres.

Cette démarche est applicable à plusieurs niveaux, de façon itérative. À haut niveau, l'opérateur va d'abord distinguer plusieurs systèmes, dont un ou plusieurs SIE, au sein de son système d'information global. Ensuite, l'opérateur va continuer à segmenter chaque SI ou SIE en distinguant des sous-systèmes. Par convention, le terme de ***sous-système*** est employé dans les deux cas.

Exemple

Ce cloisonnement doit par exemple être opéré :
- entre un SIE et des SI tiers ;
- entre un SIE et le reste du système d'information d'un opérateur ;
- entre différents SIE du même opérateur ;
- entre différents SIE devant communiquer entre eux, mais appartenant à différents opérateurs ;
- au sein de chaque SIE.

R9

⚖ Segmenter le SI en systèmes et sous-systèmes

L'opérateur doit segmenter son SI en plusieurs systèmes et ***sous-systèmes***.
Les SIE doivent être cloisonnés des autres SI de l'opérateur et des SI tiers.
Chaque SIE doit être subdivisé en sous-systèmes rassemblant des ressources assurant des fonctionnalités similaires et ayant des niveaux de ***sensibilité***, d'exposition et de sécurité homogènes.
L'opérateur doit décrire le cloisonnement mis en œuvre dans le dossier d'homologation du SIE.

Plusieurs critères permettent de décider de la manière de segmenter un SI :

- **les fonctionnalités du SI :** un SI remplit plusieurs fonctions différentes, pour des populations d'utilisateurs différentes. Le SI peut être segmenté en plusieurs sous-systèmes, chacun remplissant une fonction pour une population d'utilisateurs.
  Exemple : les environnements de développement ou de recette devraient de façon générale être séparés des environnements de production ;
- **le niveau de sensibilité :** un sous-système a des besoins particuliers de sécurité et de protection des données, exprimés suivant des critères de disponibilité, d'intégrité, de confidentialité ou de traçabilité.
  Exemple : dans un SIE constitué de plusieurs applications, les applications manipulant des données sensibles et ayant le plus fort besoin en confidentialité peuvent être regroupées et séparées des autres applications ;
- **le niveau d'exposition :** un sous-système communique avec d'autres systèmes de l'opérateur voire avec d'autres systèmes tiers. Ce sous-système doit être cloisonné des autres systèmes moins exposés afin de mettre en place des mécanismes spécifiques de défense. Le cas particulier de l'***accès à distance*** à un SIE est évoqué dans le chapitre 3.3.
  Exemple : un service Web peut être segmenté en séparant les serveurs d'application, visibles par les utilisateurs et les serveurs de base de données, visibles uniquement des serveurs d'application ;
- **le niveau de sécurité effectif :** un sous-système contenant des éléments dont le niveau de sécurité est faible est cloisonné des autres sous-systèmes.
  Exemple : les applications qui ne peuvent pas être mises à jour ou qui utilisent des protocoles dont la sécurité n'a pas été éprouvée peuvent être isolées des autres applications.

Segmenter permet de différencier les mesures de sécurité appliquées à chaque sous-système. L'opérateur évite ainsi l'écueil d'appliquer à l'ensemble d'un SIE les mesures les plus contraignantes, au risque d'imposer des exigences trop fortes à des sous-systèmes moins sensibles. À l'inverse, l'opérateur pourrait appliquer des mesures généralistes trop permissives à des sous-systèmes ayant un niveau de sensibilité particulièrement élevé.

Comme indiqué en introduction, l'objectif du cloisonnement est de réduire la surface d'attaque du SIE et les conséquences d'une atteinte à la sécurité du SIE. L'opérateur doit donc s'assurer que les interconnexions possibles entre les sous-systèmes sont strictement nécessaires.

R10

Autoriser les interconnexions suivant le besoin de fonctionnement

L'opérateur doit s'assurer que toute communication entre le SIE et d'autres SI, et entre différents sous-systèmes issus de la segmentation du SIE, est associée à un ***besoin de fonctionnement*** légitime.

Exemple

Un opérateur possède un SIE exposé sur Internet, qu'il a cloisonné en trois sous-systèmes : les serveurs d'applications, les bases de données et le SI d'administration du SIE.
Les seules interconnexions autorisées sont : d'Internet vers les serveurs d'application, des serveurs d'applications vers les bases de données, et du SI d'administration vers

les serveurs d'applications et les bases de données. Les interconnexions depuis Internet vers les bases de données ou vers le SI d'administration sont interdites.

La réflexion sur les interconnexions légitimes a bien sûr des implications sur la politique de filtrage réseau (section 3.4) mais, avant ça, cette réflexion porte également sur les choix de cloisonnement entre les sous-systèmes. Ainsi, une fois la segmentation et les interconnexions légitimes définies, l'opérateur doit concevoir et mettre en œuvre techniquement l'ensemble des mesures permettant d'aboutir à un cloisonnement adapté.

3.2.2 Cloisonnement physique ou logique

Conformément à la recommandation R9, le SI doit être cloisonné en systèmes et en sous-systèmes de sensibilité ou d'exposition similaires[14]. La présente section définit les trois types de cloisonnement et leurs propriétés de sécurité : le cloisonnement physique, le cloisonnement logique par le chiffre, et le cloisonnement logique simple. La section 3.2.3 décline ensuite ces types à différents niveaux : système, réseau et stockage.

3.2.2.1 Le cloisonnement physique

La première façon de réaliser un cloisonnement est de séparer *physiquement* les différents sous-systèmes. Ce type de cloisonnement ne met en œuvre aucun mécanisme logique. En conséquence, toute erreur de configuration ou toute exploitation de vulnérabilités qui aurait pour effet de propager une compromission à un autre sous-système est impossible[15]. C'est le type de cloisonnement le plus sûr.

R11

⚖ Mettre en place un cloisonnement physique

L'opérateur doit cloisonner physiquement des sous-systèmes de sensibilités ou d'expositions différentes et ne conserver que les interconnexions strictement nécessaires au bon fonctionnement des deux sous-systèmes.

Le terme *interconnexion* dans la recommandation s'entend au sens large. Il inclut non seulement les connexions réseau, mais aussi les possibilités de communication au sein d'un même composant physique : échanges inter processus au sein d'un système d'exploitation, communications entre plusieurs machines virtuelles à travers leur hyperviseur commun, etc.

Exemple

Quelques exemples de mise en œuvre de cloisonnement physique :

- dédier un serveur physique à des applications sensibles ;
- dédier un hyperviseur à un groupe de machines virtuelles (VM) d'un sous-système du SIE ;
- dédier des équipements (commutateurs, pare-feux) et un câblage au réseau d'un sous-système du SIE.

14. Par souci de simplification, seuls ces critères sont repris parmi les quatre cités par la recommandation R9.
15. Dans la mesure où le cloisonnement physique n'est pas aboli par l'existence d'une interconnexion par ailleurs.

3.2.2.2 Le cloisonnement logique par le chiffre

Un autre type de cloisonnement consiste en l'utilisation d'outils logiques : les sous-systèmes partagent une même ressource physique (un système, un réseau ou un support de stockage) mais un mécanisme logique organise leur cohabitation. Ce mécanisme, matériel ou logiciel, permet à l'administrateur de configurer les interconnexions autorisées entre les sous-systèmes et assure – en théorie – l'absence d'interconnexions illégitimes.

Cependant, l'efficacité du cloisonnement logique dépend de la robustesse du mécanisme logique mis en œuvre. En effet, ce mécanisme peut être défaillant, que ce soit dans sa conception ou dans sa mise en œuvre :

- erreur de configuration ;
- vulnérabilités sur le matériel ou sur le logiciel de cloisonnement ;
- présence d'un piège dans le matériel ou dans le logiciel de cloisonnement ;
- etc.

Le cloisonnement logique mis en œuvre est donc par nature d'un niveau de confiance moindre qu'un cloisonnement physique.

Une première approche du cloisonnement logique consiste à mettre en œuvre du chiffrement en amont du support physique partagé. C'est alors un ***cloisonnement (logique) par le chiffre*** : les données sont chiffrées avant d'être échangées ou stockées sur le support matériel partagé (un réseau, un moyen de stockage).

L'avantage de cette approche est que la robustesse du cloisonnement équivaut à celle du chiffrement. Le chiffrement est réalisé en amont, indépendamment des mécanismes présents sur le support physique partagé. En cas de compromission du support, un attaquant n'a accès qu'à des données chiffrées.

En général, les données du sous-système de plus forte sensibilité sont chiffrées en priorité, pour les protéger en ***confidentialité*** et en ***intégrité*** lorsqu'elles sont échangées ou stockées sur d'autres sous-systèmes. Des secrets différents, voire des mécanismes de chiffrement différents, sont recommandés pour les différents sous-systèmes à cloisonner.

R11 -

⚖ Mettre en place un cloisonnement logique par le chiffre

À défaut d'un cloisonnement physique entre sous-systèmes de sensibilités ou d'expositions différentes, l'opérateur doit avoir recours à un mécanisme logique de ***cloisonnement par le chiffre***, en utilisant des secrets différents pour les sous-systèmes à cloisonner.
L'opérateur doit s'assurer de l'efficacité du cloisonnement apporté et privilégier des solutions disposant d'un visa de sécurité de l'ANSSI.

Exemple

Exemples de mise en œuvre d'un cloisonnement logique par le chiffre :

- Les communications entre deux sous-systèmes d'un SIE doivent transiter par un réseau tiers qui n'est pas de confiance. L'utilisation d'un ***réseau privé virtuel*** (communément appelé tunnel) chiffré et authentifié cloisonne les communications du SIE des autres flux empruntant le réseau tiers.
- Un support physique de stockage est mutualisé entre un SIE et un autre SI de l'opérateur. Le chiffrement des données par le SIE avant leur écriture sur le support de stockage cloisonne ces données et les protège d'un accès par l'autre SI.

Dans ces deux exemples, un attaquant compromettant la ressource physique commune (le réseau tiers, le support de stockage) depuis un des autres SI utilisant cette ressource n'a pas accès aux informations du SIE. Cependant, cette hypothèse n'est valable que si la conception et la mise en œuvre du mécanisme de chiffrement sont robustes.

Il faut également être attentif à ce que le chiffrement soit cohérent tout au long du cycle de vie du composant. Par exemple, chiffrer les images de machines virtuelles d'un SIE lors de leur stockage protège ces images en confidentialité et en intégrité sur le stockage. Mais si ces images sont ensuite lues, déchiffrées et exécutées (en clair donc) par un hyperviseur commun au SIE et à un autre SI, alors les traitements et données du SIE ne sont plus cloisonnés par du chiffre vis-à-vis de l'autre SI.

3.2.2.3 Le cloisonnement logique simple

L'opérateur peut également envisager un ***cloisonnement*** logique simple sans chiffrement, reposant uniquement sur les capacités de cloisonnement intégrées aux solutions techniques. Le résultat est d'un niveau de sécurité minimal et un tel cloisonnement n'est pas recommandé lorsque les niveaux de sensibilité ou d'exposition sont différents.

R11 - -

⚖ Mettre en place un cloisonnement logique

À défaut d'un cloisonnement physique entre sous-systèmes ou d'un cloisonnement logique par le chiffre, l'opérateur peut avoir recours à un cloisonnement logique simple.
L'opérateur doit s'assurer de l'efficacité du cloisonnement par des mesures techniques ou organisationnelles.

Exemple

Quelques exemples d'un cloisonnement logique simple :

- Un commutateur réseau est commun à un SIE et à un autre SI. Les flux des deux SI sont cloisonnés par l'emploi de réseaux logiques virtuels (***VLAN***), sans recours à du chiffrement.
- Un réseau et une baie de stockage sont mutualisés entre un SIE et un autre SI. Des espaces logiques différents sont créés grâce aux mécanismes de *zoning* au niveau

du SAN et de *LUN masking* au niveau de la baie, contrôlant quel hôte a accès à quelle partition (cf. C.3).

- Des machines virtuelles d'un SIE et d'un autre SI partagent un même hyperviseur. L'hyperviseur assure le cloisonnement logique entre les données et traitements des différentes machines virtuelles.

Dans ces trois cas, un défaut de configuration ou une vulnérabilité dans le mécanisme logique réduisent le cloisonnement à néant.
Parmi les mesures techniques ou organisationnelles qui contribuent à s'assurer de l'efficacité d'un cloisonnement logique simple, on trouve la supervision technique ou fonctionnelle, ou la réalisation d'audits de configuration et de tests d'intrusion.

3.2.3 Mise en œuvre technique du cloisonnement

Suivant le type d'élément technique à cloisonner (système, réseau, stockage), les recommandations R11, R11- et R11-- peuvent être mises en œuvre de différentes façons. Des détails et des exemples sont donnés en annexe C.

En général, les types de cloisonnement sont combinés pour obtenir un compromis entre le niveau de sécurité (et donc de risque) et le coût de la solution.

Une attention particulière doit être portée à la mise en œuvre du cloisonnement par le chiffre pour les systèmes de stockage (et de sauvegarde).

R12

Chiffrer les données en amont du stockage avec des secrets distincts

Pour que le cloisonnement par le chiffre d'un système de stockage soit efficace, il est fortement recommandé que le chiffrement soit appliqué en amont du système de stockage, par les systèmes propriétaires des données, et non pas par le système de stockage lui-même au moment de l'écriture sur les disques.
De plus, les secrets associés au chiffrement doivent être différents pour chaque sous-système.

3.2.4 Cas des SIE dont l'hébergement est externalisé

Dans le cas particulier de SIE dont l'hébergement est externalisé, certaines entités qui externalisent n'ont pas connaissance de l'architecture mise en œuvre pour héberger leurs SIE. Il est donc nécessaire de détailler le besoin de cloisonnement afin de s'assurer que le prestataire d'externalisation n'a pas introduit une vulnérabilité en mutualisant des sous-systèmes qui devraient être cloisonnés (mutualisation au sein du SIE ou avec d'autres SI, par exemple d'autres clients).

R13

⚖ Contrôler le cloisonnement mis en place en cas d'externalisation

Dans le cas d'un SIE externalisé chez un tiers, l'opérateur doit s'assurer que son prestataire met en œuvre le cloisonnement attendu dans l'architecture proposée.

Attention

Comme indiqué dans le chapitre 2.3.3, l'opérateur est responsable d'exiger de son prestataire qu'il applique les recommandations de ce guide, puis de s'assurer que c'est effectivement fait.

3.2.5 Cas des SIE des infrastructures numériques

Les SIE du secteur des *infrastructures numériques* constituent un cas particulier. Pour rappel, selon l'annexe II de la ***directive NIS*** [1], ce secteur regroupe :

- les points d'échange Internet (*Internet exchange point* ou IXP) ;
- les fournisseurs de services DNS ;
- les registres de noms de domaine de haut niveau (*top level domains* ou TLD).

Dans ce secteur, les SIE participent directement au fonctionnement d'Internet et requièrent donc par construction une connexion directe à ce réseau, rendant les recommandations de cloisonnement difficiles à appliquer. Il est cependant recommandé de distinguer, au sein du SIE, les services, les interfaces et les flux correspondant aux services rendus (appairage de trafic, DNS) de ceux correspondant à l'administration de ces services (voir section 4.3.4) ou aux services internes au SIE (qui ne nécessitent pas une exposition à Internet).

R14

⚖ Infrastructures numériques : cloisonner les services internes

Dans le cas d'un SIE du secteur des infrastructures numériques, il est recommandé que l'opérateur applique en priorité les recommandations relatives au cloisonnement aux services internes au SIE, dont son administration.
Lorsqu'il n'est effectivement pas possible d'appliquer les recommandations précédentes sur certains de ses SIE, l'opérateur doit mettre en œuvre des mesures de protection supplémentaires afin d'atteindre les mêmes objectifs de sécurité.

Les guides techniques de l'ANSSI peuvent fournir un ensemble de bonnes pratiques au lecteur, dont les *bonnes pratiques de configuration de BGP* [19], les *bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine* [12] et les *recommandations relatives à l'interconnexion d'un système d'information à Internet* [31].

3.2.6 Cas des SIE ouverts au public

Lorsqu'un SIE est par besoin accessible depuis un réseau public comme Internet, la règle 8 exige que l'opérateur cloisonne ce SIE.

R15

⚖ Segmenter les SIE publics en au moins deux sous-systèmes

Si le SIE est accessible depuis un réseau public, l'opérateur doit segmenter le SIE en au moins deux sous-systèmes :

- un premier sous-système correspondant à la partie du SIE directement accessible depuis le réseau public. Ce sous-système joue un rôle de passerelle ;

- au moins un deuxième sous-système correspondant à la partie interne du SIE, non directement accessible depuis le réseau public mais uniquement à travers la passerelle.

L'opérateur peut se reporter au guide *recommandations relatives à l'interconnexion d'un système d'information à Internet* [31] de l'ANSSI pour concevoir la passerelle.

Comme dans tous les autres cas, mais d'autant plus lorsque le SIE est exposé sur un réseau public, le cloisonnement doit s'accompagner du filtrage des communications entre les sous-systèmes (voir section 3.4).

La segmentation en sous-systèmes d'un SIE ouvert au public est illustrée par la figure 3.3 [16]. Le SIE est segmenté en deux sous-système, « sous-SIE 1 », qui est exposé à un réseau non maîtrisé, et « sous-SIE 2 » qui ne l'est pas.

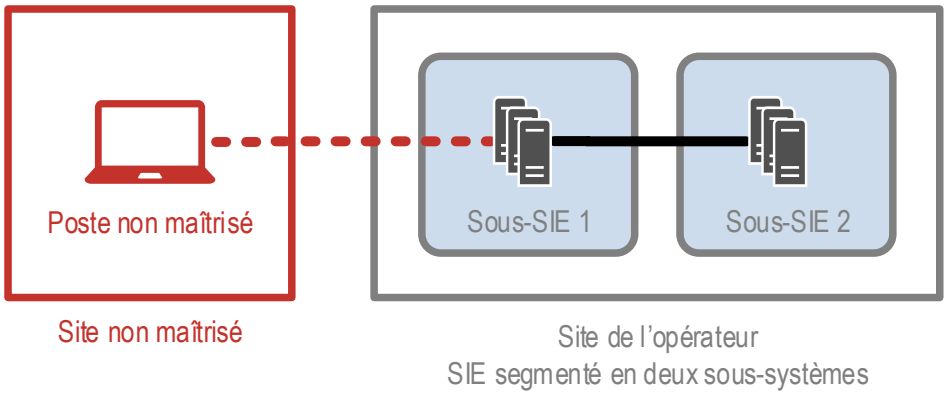

FIGURE 3.3 – SIE accessible depuis un réseau public scindé en deux sous-systèmes

Exemple

Dans le cas d'une application accessible via Internet et fournissant un service essentiel, l'opérateur peut par exemple procéder à la segmentation suivante :

- Le serveur mandataire inverse (*reverse proxy*) et le serveur Web de présentation sont placés dans le sous-système le plus exposé.
- Le serveur d'application et la base de données sont placés dans le sous-système interne.

La segmentation évoquée ci-dessus est minimale : il est recommandé de segmenter le SIE en autant de sous-systèmes que de fonctions (serveur mandataire inverse, serveur de présentation, serveur d'application, base de données) pour pouvoir filtrer finement les flux entre eux. Par exemple, si le SIE est à la fois exposé au grand public (dépôt de demandes) et à des services internes à l'entité (traitement des demandes), la segmentation des serveurs et des données et le contrôle des accès aux données doivent refléter cette organisation.

16. Sur cette figure, les moyens de filtrage ne sont pas représentés. La légende présentée page 38 s'applique également à cette figure.

3.3 Accès à distance (règle 9)

De nombreux systèmes d'information sont accessibles à distance, pour répondre à divers cas d'usage :

- service offert au grand public ou à des utilisateurs externes ;
- service offert à des utilisateurs internes mais répartis sur plusieurs sites ;
- nomadisme et ***télétravail*** ;
- maintenance à distance ;
- etc.

Objectif

Maintenir le niveau de sécurité lorsque le SIE est accédé à distance, depuis ou à travers des ressources non maîtrisées.

Accès à distance

Type d'accès dans lequel une ou plusieurs *ressources non maîtrisées* par l'opérateur sont utilisées à une quelconque étape de la connexion à un SI.
L'accès à distance est dit :

- direct, lorsqu'un utilisateur ou un serveur se connecte directement au SI cible ;
- indirect, lorsqu'un utilisateur, un serveur ou toute autre ressource se connecte en premier lieu à un autre SI avant de se connecter au SI cible.

La règle 9 énonce les exigences applicables aux situations d'accès à distance à un SIE. En effet, l'implication de ressources non maîtrisées dans l'accès à un SIE expose ce dernier à de nouvelles menaces, car les niveaux de sécurité et de confiance de ces ressources ne peuvent être vérifiés, et ne sont souvent pas à la hauteur des enjeux de sécurité du SIE. Ces ressources constituent donc des vecteurs d'attaque plus faciles à exploiter que les éléments maîtrisés par l'opérateur.

Information

L'opérateur doit décrire les mesures mises en œuvre pour protéger les accès à distance au SIE dans le dossier d'homologation du SIE.

Exemple

Exemples de ressources non maîtrisées par l'opérateur et pouvant être mises en œuvre dans l'accès à distance à un SIE :

- le poste de travail ou le terminal d'un utilisateur externe ;
- le poste de travail d'un prestataire chargé de la maintenance à distance du SIE ;
- un réseau public comme Internet ;
- un réseau dont les équipements ne sont pas directement maîtrisés par l'opérateur, tels qu'une fibre optique reliant deux sites de l'opérateur et gérée par un opérateur de communications électroniques.

Scénario d'attaque

Les utilisateurs localisés sur un site secondaire de l'opérateur accèdent au SIE à travers une liaison intersites louée à un prestataire de télécommunications. La liaison fonctionne en MPLS [17], et l'opérateur n'a pas mis en place de chiffrement.
Un attaquant réussit à compromettre le réseau du prestataire de télécommunications en exploitant une vulnérabilité sur un routeur intermédiaire. Il utilise cette compromission pour copier une partie du trafic réseau, et repère des éléments sensibles envoyés sur ce réseau comme des identifiants et mots de passe.
L'attaquant s'appuie sur ces informations pour prendre le contrôle du SIE.

Les accès à distance sont associés à des cas d'usage différents, détaillés dans les sections suivantes :

- **Les accès publics** (section 3.3.1) : le SIE est exposé à un réseau tiers comme Internet et est accessible à des utilisateurs externes (le grand public, des clients, etc.). Dans ce cas, les utilisateurs utilisent des postes non maîtrisés par l'opérateur, se connectent depuis des sites non maîtrisés (domicile, lieu public, entreprises clientes, etc.), et accèdent au SIE via un réseau non maîtrisé.
- **Les accès nomades** (section 3.3.2) : l'opérateur ouvre le SIE à un nombre limité d'utilisateurs connus (employés ou agents, prestataires). Dans ce cas, les utilisateurs emploient un poste de travail fourni par l'opérateur ou par un prestataire mandaté à cet effet, mais se connectent depuis un site non maîtrisé (domicile, cybercafé, espace de travail partagé, hôtel, etc.) et à travers un réseau non maîtrisé comme Internet. Seul le poste de travail est maîtrisé et a un niveau de sécurité connu.
- **Les accès à distance internes** (section 3.3.3) : le SIE est distribué sur plusieurs sites de l'opérateur ou l'accès au SIE est possible depuis plusieurs sites de l'opérateur. Le réseau physique transportant les flux intersites n'est pas forcément maîtrisé par l'opérateur : il peut s'agir du réseau Internet ou d'une liaison louée à un opérateur de communications électroniques. En revanche, les postes et les sites sont maîtrisés par l'opérateur.

Attention

La règle 9 précise que les accès distants au SIE par l'opérateur *ou par ses prestataires* doivent être distingués des accès par un utilisateur externe, et que ces deux premiers cas font l'objet d'exigences supplémentaires. Aussi, dans la suite de cette section, les accès distants par l'opérateur ou un prestataire doivent être considérés comme des accès *nomades* ou *internes*, et jamais comme des accès publics.

	Accès public	Accès nomade	Accès (à distance) interne
Poste de travail maîtrisé ?	**Non**	**Oui**	**Oui**
Site maîtrisé ?	**Non**	**Non**	**Oui**
Réseau maîtrisé ?	**Non**	**Non**	**Non**

FIGURE 3.4 – Caractérisation des accès distants en fonction de la maîtrise des ressources utilisées

17. MPLS : *multiprotocol label switching*, technologie réseau qui permet d'acheminer sur une unique infrastructure différents types de trafic tout en les isolant.

Les schémas présentés par la suite utiliseront la légende présentée dans la figure 3.5 :

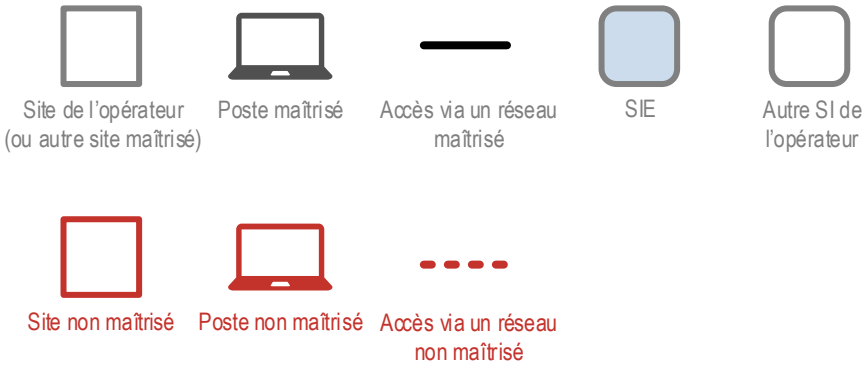

FIGURE 3.5 – Légende des schémas relatifs aux accès distants

3.3.1 Accès publics à un SIE

Dans le cas des accès publics à un SIE, l'accès se fait à partir et à travers des environnements (poste, site, réseau) que l'opérateur ne maîtrise pas et qu'il ne peut donc considérer comme étant de confiance. On rencontre ce cas pour des applications Web ouvertes au public ou à des utilisateurs connus mais externes. L'accès peut être direct ou indirect, comme illustré dans la figure 3.6.

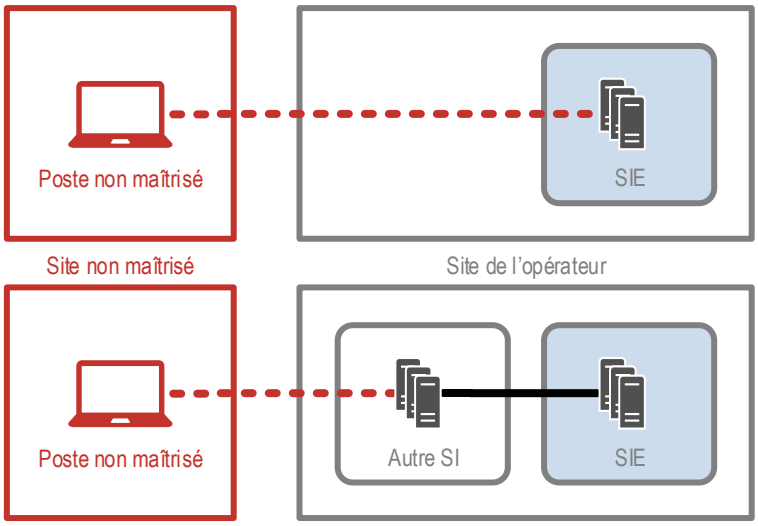

FIGURE 3.6 – Accès public direct et indirect à un SIE

Les services hébergés sur des SIE ouverts au public présentent la particularité d'être accessibles depuis des équipements dont le niveau de sécurité n'est pas maîtrisé par l'opérateur. Cependant, la politique d'accès au SIE peut imposer des mesures concernant la sécurité des communications et l'authentification des utilisateurs, et enfin nécessiter de se protéger sans présupposer des caractéristiques des postes ou serveurs qui s'y connectent.

Ainsi, la mise en œuvre de ***cloisonnement logique par le chiffre*** est limitée par l'absence de maîtrise du poste de l'utilisateur : l'opérateur ne peut pas s'appuyer sur un logiciel client particulier pour imposer un tunnel IPsec ou ***TLS***. En revanche, il est possible de mettre en œuvre, à l'initiative du SIE, du chiffrement applicatif (HTTPS par exemple) et l'authentification des utilisateurs.

R16

⚖ Accès public : chiffrer et authentifier les flux au niveau applicatif

L'opérateur doit mettre en œuvre un ***cloisonnement logique par le chiffre*** pour l'accès public au SIE, en utilisant si nécessaire des protocoles ne nécessitant pas d'installer d'éléments sur le poste de l'utilisateur. Cela inclut l'utilisation du protocole HTTPS pour les accès Web.
Il est fortement recommandé que ces protocoles soient conformes aux règles préconisées par l'ANSSI et détaillées notamment dans le *référentiel général de sécurité* [34] et dans les *recommandations de sécurité relatives à TLS* [28].
Il est également fortement recommandé que le SIE soit authentifié par la présentation d'un certificat serveur dont les clients peuvent vérifier la validité.

R17

Accès public : authentifier les utilisateurs

Il est fortement recommandé que tout élément du SIE accessible publiquement et qui nécessite une authentification de l'utilisateur fasse appel à un mécanisme d'authentification à l'état de l'art.

R17 +

Accès public : authentifier les utilisateurs avec deux facteurs

Si le besoin de sécurité le justifie, il est fortement recommandé de mettre en place une ***authentification à double facteur*** pour les utilisateurs du service.

Ces mesures renforcent la confiance dans l'intégrité et la confidentialité des informations échangées entre le SIE et les utilisateurs. En revanche, ces mesures ne diminuent pas l'exposition du SIE : celui-ci reste exposé à des attaques génériques ou ciblées venant d'Internet. Il est donc nécessaire de renforcer la sécurité de l'interconnexion entre le SIE et Internet.

La première mesure est de cloisonner le SIE en au moins deux parties, externe et interne, comme exigé par la recommandation R15 dans la section 3.2 sur le cloisonnement. Le lecteur peut se reporter aux *recommandations relatives à l'interconnexion d'un système d'information à Internet* [31].

D'autres mesures, présentées dans la suite de ce guide, sont également applicables en priorité à la partie externe d'un SIE exposé sur Internet : le filtrage des accès, détaillé en section 3.4, et le maintien en conditions de sécurité, objet du chapitre 6.

3.3.2 Accès nomades à un SIE

Dans le cadre de ce guide, nous considérons l'utilisateur nomade comme un utilisateur légitime du SIE ayant un poste de travail maîtrisé, mais accédant au SIE depuis un site non maîtrisé et via un réseau non maîtrisé. L'utilisateur peut-être un employé ou un agent de l'opérateur, ou bien un prestataire mandaté par l'opérateur. Ce cas est illustré par la figure 3.7.

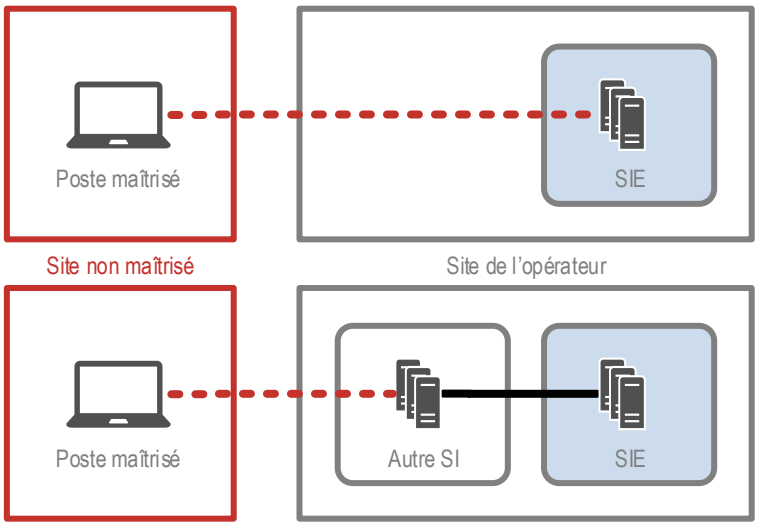

FIGURE 3.7 – Accès nomade direct ou indirect à un SIE

Scénario d'attaque

Un utilisateur nomade est doté d'un poste de travail dont le niveau de sécurité est maîtrisé par l'opérateur. Cependant, les attaques suivantes restent possibles :

- un attaquant compromet le réseau employé par l'utilisateur afin d'écouter les communications et récupère des éléments d'authentification relatifs au SIE ;
- un attaquant vole le poste de travail et en extrait de l'information concernant le SIE (par exemple, des informations de connexion) ;
- un attaquant vole le poste de travail et accède au SIE ;
- un attaquant à proximité dans un lieu public observe les touches tapées par l'utilisateur et les informations affichées sur l'écran et aperçoit des mots de passe ou des informations concernant le SIE.

Pour les situations de mobilité, l'opérateur peut dans un premier temps se référer aux *bonnes pratiques à l'usage des professionnels en déplacement* [15] de l'ANSSI, puis aux *recommandations sur le nomadisme numérique* [26] pour augmenter le niveau de sécurité des situations de nomadisme. Parmi toutes les recommandations de ce dernier guide, certaines sont à considérer en priorité et sont reprises ci-dessous. Leur mise en œuvre permet de lutter notamment contre les exemples d'attaques précédents.

Lors d'un accès nomade, l'opérateur maîtrise le poste de l'utilisateur et peut requérir l'installation d'éléments matériels ou logiciels de chiffrement de flux.

R18

⚖ Accès nomade : mettre en place un tunnel chiffré et authentifié

L'opérateur doit configurer le poste de travail nomade afin qu'il établisse toujours un tunnel authentifié et chiffré depuis le poste de travail jusqu'au SIE, ou à défaut, jusqu'au SI interne de l'opérateur.

Il est recommandé de mettre en œuvre un tunnel reposant sur la technologie de ***VPN IPsec***, configuré conformément aux *recommandations de sécurité relatives à IPsec pour la protection des flux réseau* [24] de l'ANSSI. À défaut, la technologie TLS peut être employée [28].

La mise en œuvre de cette recommandation avec un tunnel à l'état de l'art établit un ***cloisonnement par le chiffre*** des communications entre le poste de travail et le SIE (ou le SI de l'opérateur), et permet d'obtenir le même niveau de confidentialité, d'intégrité et de robustesse d'authentification que pour des accès via un réseau maîtrisé.

Le tunnel doit couvrir l'ensemble des communications. Ainsi, l'utilisateur ne doit pas pouvoir désactiver temporairement le tunnel (pour se connecter au portail captif d'un hôtel par exemple), ni pouvoir accéder directement à Internet ou communiquer avec un équipement sur le réseau local (imprimante personnelle à domicile). Le lecteur peut se reporter aux *recommandations sur le nomadisme numérique* [26, chapitre 3.4] pour les détails de mise en œuvre.

Cependant, l'accès se fait toujours depuis un site non maîtrisé. Les mesures suivantes visent à mieux protéger le poste de l'utilisateur dans cette situation de nomadisme : renforcement de l'authentification, de la confidentialité et de l'intégrité des informations affichées ou stockées sur le poste.

R19

⚖ Accès nomade : authentifier les utilisateurs avec deux facteurs

L'opérateur doit s'assurer de l'identité de l'utilisateur nomade en l'obligeant à utiliser une ***authentification à double facteur*** sur le poste de travail.
Lorsque des raisons techniques ou organisationnelles empêchent de mettre en place de l'authentification à double facteur pour les utilisateurs nomades, l'opérateur doit décrire ces raisons dans le dossier d'homologation du SIE.

R20

⚖ Accès nomade : chiffrer intégralement le disque du poste

L'opérateur doit protéger la confidentialité et l'intégrité des mémoires de masse utilisées sur les postes de travail en les chiffrant intégralement (à la fois la partition système et les partitions de données).
L'opérateur doit employer des mécanismes de chiffrement et d'authentification conformes aux règles préconisées par l'ANSSI et détaillées notamment dans le *Référentiel général de sécurité (RGS)* [34].

R21

Accès nomade : utiliser des filtres de confidentialité

Il est fortement recommandé que l'opérateur fournisse aux utilisateurs en situation de nomadisme des filtres de confidentialité, afin de protéger la confidentialité des données relatives au SIE.

Attention

Quelles que soient les mesures de sécurité mises en œuvre, il est recommandé d'inciter l'utilisateur nomade à déclarer sans délai le vol ou la perte de son poste

de travail. L'opérateur peut ainsi prendre les mesures d'exclusion nécessaires et bloquer les potentielles tentatives d'accès d'un attaquant au SIE.

3.3.3 Accès internes à un SIE

Les accès à distance dits « internes » couvrent les accès au SIE depuis des équipements maîtrisés par l'opérateur (des postes de travail, des serveurs ou d'autres SI), localisés sur un site maîtrisé par l'opérateur, mais à travers un réseau qui n'est pas maîtrisé par l'opérateur. Ce cas couvre également un SIE réparti sur plusieurs sites de l'opérateur.

Un accès interne peut prendre différentes formes, notamment celles rappelées dans les figures 3.8 et 3.9 :

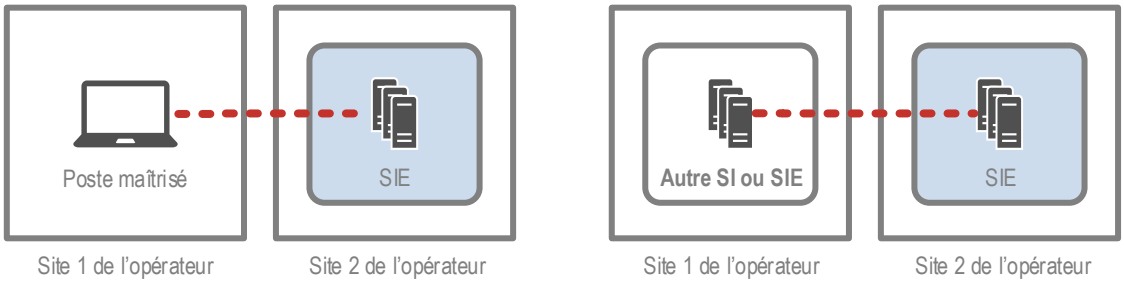

FIGURE 3.8 – Accès internes directs d'un poste ou d'un serveur à un SIE

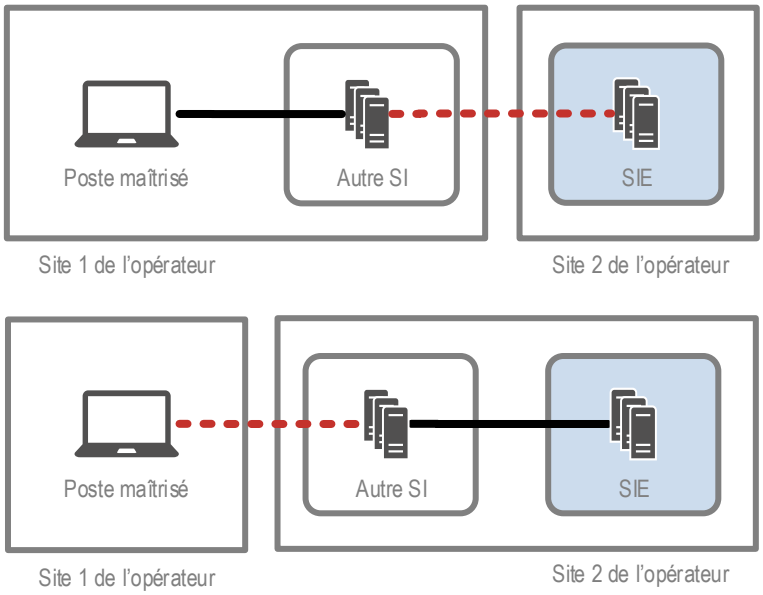

FIGURE 3.9 – Accès internes indirects d'un poste à un SIE depuis un site distant

La présence d'un réseau non maîtrisé permettant d'accéder à un SIE expose ce dernier à des accès illégitimes, et crée aussi un risque pour la confidentialité et l'intégrité des données échangées.

Le vecteur d'attaque que constitue un réseau non maîtrisé doit donc être désactivé en mettant en œuvre, comme pour les recommandations R16 et R18, un ***cloisonnement par le chiffre*** des communications réseau afin de se retrouver dans des conditions de sécurité équivalentes à celles d'un réseau maîtrisé par l'opérateur.

R22

⚖ Accès interne : mettre en place un tunnel chiffré et authentifié

L'opérateur doit mettre en place un tunnel authentifié et chiffré dès lors qu'une communication liée au SIE transite par un réseau non maîtrisé.
Il est recommandé de mettre en œuvre un tunnel reposant sur la technologie de ***VPN IPsec***, configuré conformément aux *recommandations de sécurité relatives à IPsec pour la protection des flux réseau* [24] de l'ANSSI. À défaut, la technologie TLS peut être employée [28].

Comme pour la R18, le tunnel doit couvrir l'ensemble des communications. Le lecteur peut se reporter aux *recommandations sur le nomadisme numérique* [26, chapitre 3.4] pour les détails de mise en œuvre.

3.4 Filtrage réseau (règle 10)

Filtrage

Démarche visant à autoriser ou interdire des actions en fonction de règles préétablies ou construites automatiquement.

Objectif

S'assurer que seuls sont autorisés les flux réseau nécessaires au bon fonctionnement du SIE ou à sa sécurité, en filtrant ces flux.

La règle 10 exige des mécanismes de ***filtrage*** pour compléter le cloisonnement requis par la règle 8 (section 3.2). En application du principe de ***besoin de fonctionnement***, un utilisateur ou un processus automatique n'ayant pas besoin d'accéder à un élément du SIE doit voir toute tentative d'accès (volontaire ou involontaire) à cet élément bloquée. Pour cela, il faut mettre en place une série de dispositifs techniques, au premier rang de laquelle se trouve le filtrage réseau.

Scénario d'attaque

L'opérateur met en œuvre différents SI cloisonnés entre eux, dont le SI bureautique et un SIE. Chaque système dispose d'un ou plusieurs sous-réseaux logiques (VLAN), mais l'opérateur n'a pas mis en œuvre de filtrage entre ces sous-réseaux.
Un attaquant compromet d'abord un poste de travail au moyen d'un courriel piégé. En l'absence de filtrage réseau et de cloisonnement physique, l'attaquant effectue une cartographie du réseau et découvre les sous-réseaux associés au SIE. Il effectue ensuite un ***déplacement latéral*** vers une ressource du SIE.

Pour mettre en œuvre le filtrage réseau, il est recommandé de suivre une démarche en 4 étapes :

- définir l'emplacement des points de filtrage (section 3.4.1) ;
- définir le besoin de filtrage en s'appuyant sur le ***besoin de fonctionnement*** (section 3.4.2) ;
- traduire le besoin de filtrage en règles (section 3.4.3) ;
- mettre en œuvre le filtrage en implémentant les règles sur les dispositifs (section 3.4.4).

Information

L'opérateur doit décrire les mécanismes de filtrage mis en place dans le dossier d'homologation du SIE.

3.4.1 Points de filtrage

Dans la section 3.2 consacrée au cloisonnement, les recommandations R9 et R10 demandent de segmenter le système d'information de l'opérateur en systèmes et sous-systèmes distincts [18].

18. Si la règle ne s'applique formellement qu'aux SIE, cette bonne pratique a vocation a être déclinée sur l'ensemble du SI de l'opérateur : le cloisonnement et le filtrage restent, dans la plupart des cas, des éléments fondateurs d'un système de défense en profondeur.

Les interconnexions entre les systèmes et entre les sous-systèmes sont les *points de filtrage principaux*, les points auxquels les dispositifs de filtrage sont mis en œuvre.

R23

⚖ Filtrer les flux aux interconnexions entre les systèmes et entre les sous-systèmes

L'opérateur doit filtrer les flux réseau au niveau des interconnexions entre les systèmes et les sous-systèmes définis par la règle 7 relative au cloisonnement. Ce filtrage est désigné *filtrage périmétrique*.
Les dispositifs de filtrage périmétrique ne peuvent être mutualisés qu'entre des sous-systèmes de sensibilité et d'exposition similaires.

Le principe de défense en profondeur conduit à compléter le filtrage périmétrique effectué sur les données en transit par du filtrage local aux extrémités des flux – en général des serveurs ou des postes de travail. Le filtrage local répond à deux objectifs :

- doubler le filtrage périmétrique en filtrant à nouveau les communications au niveau de chaque équipement d'extrémité ;
- ajouter du filtrage entre les équipements au sein d'un sous-système.

Les équipements d'extrémité sont donc des *points de filtrage secondaires*.

R23 +

Filtrer les flux aux extrémités des communications

En complément du filtrage périmétrique, il est recommandé de filtrer les flux aux extrémités des communications, au niveau des serveurs, postes de travail et autres équipements. Ce filtrage est désigné *filtrage local*. Il est en général mis en œuvre par des pare-feux logiciels intégrés aux équipements.

Le complément apporté par le filtrage local est d'autant plus important que les sous-systèmes ont été définis de façon large. Le filtrage local limite alors les déplacements latéraux d'un attaquant au sein d'un sous-système comprenant un grand nombre d'éléments.

Une fois définis les points de filtrage, l'opérateur doit formaliser les besoins de filtrage à chaque point.

3.4.2 Besoins de filtrage

Les flux réseau sont filtrés et autorisés relativement au ***besoin de fonctionnement*** du SIE. Ce besoin tient compte des flux nécessaires au service métier rendu par le SIE et de ceux nécessaires à sa sécurité. Le besoin de fonctionnement peut être exprimé en termes fonctionnels par les équipes responsables de la conception de chaque SIE.

R24

⚖ Définir les besoins de filtrage sur le SIE

L'opérateur doit répertorier précisément les communications strictement nécessaires (ou ***besoin de fonctionnement***) entre le SIE et les autres systèmes, et entre les sous-systèmes du SIE, pour formaliser les besoins de filtrage.

Attention

Dans le cas particulier d'un SIE nécessaire à la fourniture de service d'interconnexion par appairage pour l'échange de trafic Internet [19], l'opérateur ne met en place des mécanismes de filtrage que pour les flux de données autres que ceux correspondant au trafic Internet proprement dit.

3.4.3 Règles de filtrage

Une fois les besoins de filtrage établis, il faut les décliner en une liste de règles techniques de filtrage, règles qui seront ensuite implémentées dans les dispositifs de filtrage. Une granularité fine sera recherchée pour le filtrage des flux, au moins pour les SI les plus sensibles.

Scénario d'attaque

Lors d'un dépannage sur le SIE, un flux a été autorisé pour administrer une application à travers un protocole non chiffré, puis laissé autorisé alors qu'il n'est plus nécessaire. L'opérateur n'organise pas de revues régulières de ses règles de filtrage et ne s'aperçoit pas de cet écart.
Un attaquant utilise cette opportunité pour s'introduire dans le SIE depuis un poste de travail compromis.

R25

Formaliser les règles de filtrage

L'opérateur doit établir et tenir à jour une liste des règles de filtrage en vigueur et des règles supprimées depuis moins d'un an. Cette liste constitue la matrice de flux globale.

Il est fortement recommandé que cette liste précise pour chaque règle :

- la date et le motif de la mise en œuvre, de la modification ou de la suppression de la règle ;
- un historique daté des modifications de la règle ;
- les modalités techniques de mise en œuvre de la règle, notamment le point de filtrage (le dispositif de filtrage) concerné ;
- les critères techniques de filtrage réseau : adresses réseau, protocoles, numéros de ports, modes d'inspection, etc.

Le respect de ce formalisme permet de revoir plus facilement les règles lors des analyses *a posteriori*. En effet, pour que le filtrage soit efficace, il faut que sa formalisation soit maintenue dans le temps pour :

- supprimer les règles devenues obsolètes ;
- vérifier que tous les éléments attendus sont bien précisés et pertinents : raisons de création, modification ou suppression des règles, éléments techniques ;
- tracer les fusions et les optimisations de règles pour des raisons techniques ou de performance ;

19. IXP ou *Internet exchange point*.

- détecter et corriger les écarts : d'une part, les écarts entre ce qui est attendu, notamment au vu de la ***PSSI***, et ce qui est formalisé par les règles ; d'autre part, les écarts entre ce qui est formalisé par les règles et ce qui est implémenté sur les dispositifs de filtrage.

R26

Passer régulièrement en revue les règles de filtrage

Il est recommandé que l'opérateur effectue régulièrement une revue exhaustive des règles de filtrage relatives au SIE afin de s'assurer que ce qui est attendu est pertinent, et que ce qui est implémenté correspond effectivement à ce qui est attendu.
La périodicité de cette revue est fixée par l'analyse de risque, mais il est recommandé qu'elle ne dépasse pas un an.

Sans cette revue régulière des règles de filtrage, il est souvent observé une dérive des règles : écart entre les règles formalisées et les règles implémentées, manque de rigueur dans les descriptions des règles et de leurs modifications.

Information

Deux guides de l'ANSSI peuvent accompagner les recommandations R25 et R26 :
- *Définition d'une politique de pare-feu* [21] ;
- *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu* [25].

3.4.4 Mise en œuvre du filtrage

Après avoir formalisé les règles de filtrage, il faut les mettre en œuvre à l'aide de dispositifs techniques de filtrage, afin de n'autoriser effectivement que les flux nécessaires et d'interdire tous les autres.

3.4.4.1 Choix et mutualisation des dispositifs de filtrage

Les dispositifs incluant une fonction de filtrage peuvent être de natures différentes :

- pare-feu réseau ;
- pare-feu local d'un serveur ou d'un poste de travail ;
- liste de contrôle d'accès (***ACL***) sur un routeur ;
- serveur mandataire (***proxy***) effectuant une rupture de flux ;
- diode garantissant l'unidirectionnalité d'un flux ;
- etc.

Si toutes ces approches sont intéressantes, il est néanmoins fortement recommandé d'utiliser des dispositifs spécialement conçus pour effectuer une fonction de filtrage afin d'avoir l'assurance que ce filtrage est effectivement bien réalisé.

R27

Mettre en œuvre le filtrage grâce à des équipements spécialisés

Il est fortement recommandé que l'opérateur utilise des dispositifs dédiés tels que des pare-feux pour mettre en œuvre la fonction de filtrage, et non des équipements dont ce n'est pas la fonction première.
Il est recommandé de privilégier des solutions disposant d'un visa de sécurité de l'ANSSI.
Enfin, dans un objectif de réduction de la surface d'attaque, il est recommandé que l'opérateur limite le nombre de fonctions [20] portées par ses pare-feux.

Attention

Il est préférable de ne pas recourir à un routeur avec des listes de contrôles d'accès (ACL) pour remplir une fonction de filtrage. En effet, les ACL fonctionnent avec un mode « sans état » et ne peuvent donc pas servir à filtrer efficacement une session [21].
Il est recommandé de choisir des pare-feux mettant en œuvre un suivi dynamique des sessions (pare-feux dits avec état ou *stateful*) et d'activer cette fonctionnalité.

Par ailleurs, le principe du cloisonnement décrit en section 3.2 s'applique également aux dispositifs de filtrage eux-mêmes : les dispositifs de filtrage associés à des sous-systèmes de sensibilité ou d'exposition différentes doivent être cloisonnés, c'est-à-dire être physiquement ou à défaut logiquement distincts.

Exemple

Un SIE est exposé sur Internet. Le SIE est divisé en trois sous-systèmes : les services relais servant de passerelle avec Internet, les services internes comme les bases de données, et les postes de travail des utilisateurs internes chargés du traitement des demandes.
Le dispositif de filtrage contrôlant les flux entre Internet et les services relais est bien plus exposé que celui contrôlant les flux entre les services relais, les services internes et les postes des utilisateurs internes. Il est donc recommandé d'utiliser des dispositifs de filtrage distincts.
Cet exemple est illustré par la figure 3.10. Il est inspiré par le chapitre 2.4 « Architecture détaillée » du guide *recommandations relatives à l'interconnexion d'un système d'information à Internet - v2.0* [31] de l'ANSSI.

20. Les deux fonctions principales sont le filtrage réseau et le filtrage applicatif, à répartir sur des équipements distincts. Les fonctions annexes nécessaires sont la journalisation et la gestion des politiques de filtrage. D'autres fonctions sont parfois proposées, mais il est recommandé de les déporter sur d'autres équipements que les pare-feux : détection de codes malveillants ou détection d'intrusion (IDS), serveur mandataire, terminaison de tunnel VPN, équilibrage de charge, etc.
21. Par exemple, un filtrage sans état ne permet pas d'autoriser certains paquets entrants uniquement après l'ouverture d'une connexion par une source interne.

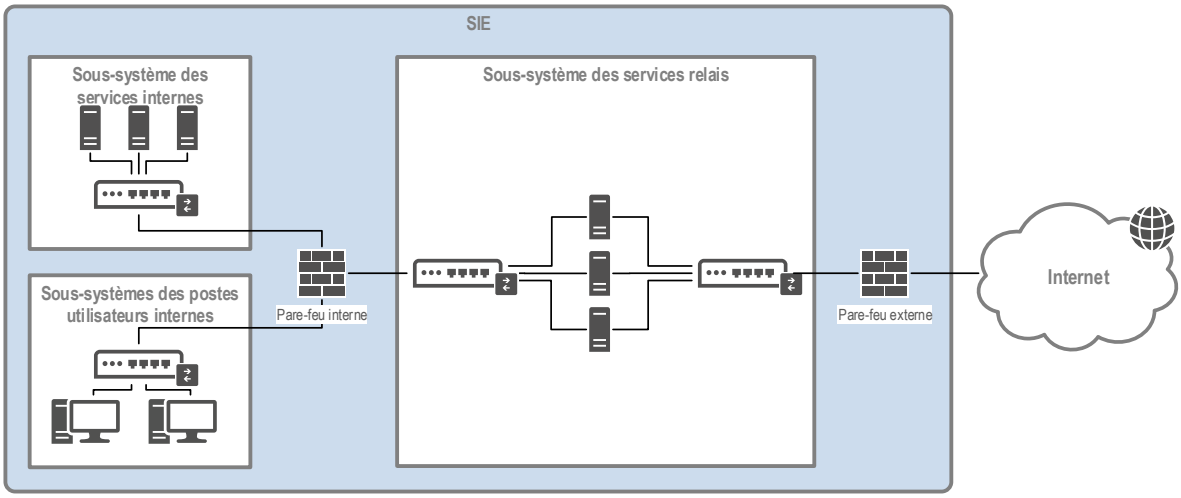

FIGURE 3.10 – Exemple de cloisonnement physique des dispositifs de filtrage

3.4.4.2 Listes d'autorisation et d'interdiction

Les dispositifs de filtrage fonctionnent selon deux principes :

- la ***liste d'autorisation*** (*allow list* ou encore liste blanche) : on décrit les flux qui sont spécifiquement autorisés et tous les autres sont strictement interdits ;
- la ***liste d'interdiction*** (*deny list* ou encore liste noire) : on décrit les flux qui sont spécifiquement interdits et tous les autres sont autorisés par défaut.

La liste d'autorisation a l'avantage d'être plus explicite dans ce qui est autorisé et donc de ne pas limiter les flux potentiellement malveillants à une liste prédéfinie. Ainsi, une attaque qui ne serait pas encore connue sera quand même bloquée. En revanche, cette approche demande de bien connaître son besoin de fonctionnement et de faire évoluer sa matrice de flux au fur et à mesure de l'évolution du besoin.

Par ailleurs, la règle 10 sur le filtrage exige que « les flux qui ne sont pas conformes aux règles de filtrage [soient] bloqués par défaut ».

R28

⚖ Bloquer tous les flux non explicitement autorisés

L'opérateur doit mettre en œuvre des mécanismes de filtrage reposant sur le principe des ***listes d'autorisation***, en décrivant spécifiquement ce qui est autorisé et en interdisant par défaut tous les autres flux.

4
Sécurité de l'administration (règles 11 et 12)

Ce chapitre détaille les recommandations relatives à la section 2 du chapitre II de l'*arrêté du 14 septembre 2018*. Il couvre les règles relatives aux comptes d'administration (règle 11) et aux systèmes d'information d'administration (règle 12).

En application du principe de cloisonnement décrit dans la règle 8 et dans la section 3.2, ce chapitre propose une segmentation entre les actions (section 4.1), les comptes et les privilèges (section 4.2), et les ressources matérielles et logicielles (section 4.3) d'utilisation courante et celles relatives à l'administration du SIE.

Information

L'ANSSI a publié un guide de recommandations relatives à l'*Administration sécurisée des systèmes d'information* [27]. Le présent chapitre reprend de façon succincte les notions et recommandations issues de ce guide. Il est fortement recommandé au lecteur de consulter ce guide pour avoir plus précisions, et de mettre en œuvre sur ses SI d'administration l'intégralité des recommandations du guide.

4.1 Actions d'administration

Objectif

Identifier les actions susceptibles d'altérer le fonctionnement ou la sécurité du SIE pour en garantir une utilisation légitime.

Action d'administration

Action d'installation, de consultation, de modification ou de suppression d'un composant d'un SI susceptible de modifier le fonctionnement ou la sécurité de celui-ci.

Par définition, les actions d'administration sont des vecteurs d'attaque importants sur un SI, puisqu'un attaquant peut les utiliser pour compromettre le fonctionnement ou la sécurité du SI. L'opérateur doit donc identifier précisément ce que sont les actions d'administration avant de protéger les comptes et les ressources associés à ces actions.

L'identification des ***actions d'administration*** applicables au SIE est recommandée, pour ensuite protéger l'accès à ces actions. Quelques exemples non exhaustifs d'actions d'administration :

- installation de micro-codes, de systèmes d'exploitation, de logiciels ;
- configuration de matériels et de logiciels, et en particulier ceux relatifs à la sécurité du SI ;
- gestion des comptes, des privilèges et des droits d'accès, par exemple à travers un annuaire ;
- programmation d'un automate industriel ;
- maintenance et supervision, dès lors que ces actions nécessitent des privilèges de même niveau que pour effectuer les actions d'administration.

Information

Il est parfois pertinent de distinguer l'administration *technique* de l'administration *métier*. Cette dernière correspond à la gestion fine des droits au sein d'une application métier particulière (permissions des utilisateurs au sein de l'application). Le périmètre d'action et les privilèges d'un administrateur métier sont limités à une application.
L'application des recommandations de ce chapitre aux administrateurs métier doit être modulée en fonction des privilèges dont ils disposent, des risques induits pour la sécurité du SIE et enfin des possibilités techniques offertes par l'application (outil d'administration métier distinct de l'outil offert aux utilisateurs, par exemple).
Dans tous les cas, tous les comptes d'administration, techniques comme métiers, sont des ***comptes privilégiés***, soumis aux recommandations des sections 5.2.2.1 et 5.3.1.

4.2 Comptes d'administration (règle 11)

Les comptes utilisés pour les actions d'administration sont particulièrement sensibles car ils donnent aux administrateurs :

- des privilèges élevés sur les ressources à administrer ;
- un accès aux outils d'administration ;
- la capacité de modifier le comportement des mesures de sécurité.

Objectif

S'assurer de la légitimité d'une personne à exécuter des ***actions d'administration*** et garantir la traçabilité de ses actions en utilisant des comptes spécifiques, les ***comptes d'administration***.

La règle 11 demande de mettre en œuvre des comptes dédiés aux actions d'administration et de gérer ces comptes en respectant des exigences particulières. La présente section détaille comment répondre à ces exigences (section 4.2.1), puis comment protéger les comptes d'administration (section 4.2.2).

4.2.1 Usage des comptes d'administration

La protection des comptes d'administration commence par une définition précise de leur cadre d'utilisation, par leur identification et leur bonne gestion.

Scénario d'attaque

L'administrateur d'un SIE utilise un seul compte pour naviguer sur Internet et pour administrer le SIE. Ce compte n'est pas protégé par une authentification à double facteur.
Un attaquant cible l'administrateur avec une attaque par hameçonnage et le conduit à donner son mot de passe sur un site Web illégitime. L'attaquant dispose alors de secrets d'authentification pour accéder au SIE en tant qu'administrateur.

Les actions d'administration doivent être effectuées depuis des comptes dédiés à ce type d'action, et seules ces actions d'administration peuvent être faites depuis ces comptes.

R29

⚖ Utiliser des comptes d'administration dédiés

L'administrateur doit disposer d'un ou plusieurs comptes d'administration dédiés, distincts de son compte utilisateur, pour effectuer des actions d'administration.
Les comptes d'administration doivent être utilisés *exclusivement* pour des actions d'administration. En particulier, aucun ***compte d'administration*** ne doit être utilisé pour des actions bureautiques ou l'ouverture de sessions de travail sur des postes autres que ceux réservés aux actions d'administration.

Information

Il est recommandé d'appliquer une convention de nommage claire pour distinguer simplement les comptes d'administration des autres comptes, et pour vérifier la bonne ségrégation de leurs usages. Le lecteur peut consulter les exemples du chapitre 7.1 du guide *Administration sécurisée des systèmes d'information – v2.0* [27].

Dans certains cas, l'administration d'une ressource ne peut pas techniquement être effectuée à partir d'un compte spécifique d'administration. L'opérateur doit alors atteindre par d'autres moyens l'objectif de protection des actions d'administration : traçabilité et supervision des actions d'administration, actions d'administration effectuées exclusivement par des administrateurs, limitation des adresses IP, etc.

Exemple

Sur certains équipements, toutes les opérations sont accessibles à tous les utilisateurs, sans notion de privilège. Dans d'autres cas, les équipements ne gèrent pas de comptes.

R29 -

⚖ Pallier l'absence de comptes dédiés à l'administration

Lorsque des raisons techniques empêchent d'utiliser des comptes dédiés à l'administration, l'opérateur doit mettre en place d'une part des mesures permettant d'assurer la traçabilité et le contrôle des actions d'administration réalisées sur cette ressource et d'autre part des mesures de réduction du risque lié à l'utilisation d'un compte qui n'est pas dédié à l'administration.

L'opérateur doit décrire les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.

La justification de l'exception doit se faire sur des critères uniquement techniques. Ainsi, l'utilisation d'un même compte pour les actions d'administration et pour d'autres actions n'est pas acceptable si une solution technique existe.

L'utilisation d'un compte sur un élément de SI laisse potentiellement des traces qui peuvent être utilisées par un attaquant pour compromettre le compte associé. L'utilisation des comptes d'administration doit donc être limitée aux équipements pour lesquels l'administrateur a des actions à réaliser. Un compte d'administrateur ne doit donc pas servir à ouvrir une session bureautique sur un poste de travail. Ainsi, cette spécialisation et la réduction de l'usage des comptes d'administrations contribuent à diminuer la probabilité qu'ils soient compromis.

Les actions non relatives à l'administration (navigation sur Internet, messagerie, bureautique, accès applicatifs métier, etc.) doivent être faites depuis un compte utilisateur et jamais depuis un compte d'administration. Les administrateurs disposent donc en général d'au moins deux comptes : un compte utilisateur et un ou plusieurs comptes d'administration, et les secrets d'authentification de tous ces comptes doivent être distincts.

Par ailleurs, les comptes natifs d'administration, dits *built-in* (ex. : root, admin), présents par défaut sur les équipements lors de l'installation ne doivent pas être utilisés. Leur utilisation doit rester exceptionnelle et restreinte à un nombre d'administrateurs très limité. En effet, ces comptes ne permettent pas d'imputer de manière précise les actions effectuées sur les équipements. Cela rend aussi impossible la mise en œuvre d'un contrôle d'accès pertinent aux outils d'administration et la ségrégation des droits. Seule la création de comptes individuels d'administration peut répondre à ces besoins.

Rappel : lorsqu'ils existent, les mots de passe par défaut des comptes natifs doivent être changés au titre de la recommandation R1.

R30

⚖ Utiliser par défaut des comptes d'administration individuels

L'opérateur doit créer un compte d'administration individuel pour chaque administrateur.
Les comptes *natifs* d'administration ne doivent pas être utilisés pour les actions courantes d'administration et les secrets associés ne doivent être accessibles qu'à un nombre très restreint de personnes.

Enfin, la règle 11, en complément de la règle 6 sur la cartographie, impose à l'opérateur d'établir et de tenir à jour une liste des comptes d'administration. Cette exigence est présentée en tant que recommandation R56 dans la section 5.3.1.

Information

Le système d'information d'administration d'un SIE n'est pas forcément inclus dans le périmètre du SIE, ou n'est pas forcément désigné en tant que SIE lui-même. Cependant, les administrateurs d'un SIE sont considérés comme des utilisateurs de ce SIE.

À ce titre, les règles sur l'identification, l'authentification et la gestion des droits d'accès énoncées au chapitre 5 s'appliquent aux comptes d'administration.

Pour faciliter la gestion des droits d'administration (ajout, modification et suppression), il est recommandé de créer des groupes dans le ou les annuaires des comptes d'administration. Un groupe contient, en fonction du juste besoin opérationnel, l'ensemble des comptes d'administration devant disposer de droits d'administration homogènes sur une ou plusieurs ressources administrées. Les droits sur ces ressources sont ainsi octroyés aux groupes et non aux comptes.

R31

Attribuer les droits d'administration à des groupes

Il est recommandé d'attribuer les droits d'administration à des groupes de comptes d'administration plutôt qu'unitairement à des comptes d'administration.

4.2.2 Protection des comptes d'administration

Les actions d'administration sont effectuées au moyen de ***comptes d'administration*** individuels, relatifs à des personnes physiques ou à des processus automatiques. Ces comptes sont vulnérables aux attaques classiques sur les comptes utilisateur, mais avec un impact potentiel plus important.

Scénario d'attaque

Un administrateur a utilisé le mot de passe `adminpassword` pour le compte root d'un serveur sous Linux.
Un attaquant lance une attaque en force brute pour se connecter au compte root, en utilisant un dictionnaire de mots de passe. Il retrouve facilement le mot de passe, compromet le compte d'administration et prend le contrôle du serveur.

La protection des comptes d'administration représente donc un enjeu important et demande la mise en œuvre de mesures particulières.

Les annuaires contribuant à identifier et authentifier les administrateurs sur les ressources administrées sont des éléments critiques. Leur prise de contrôle par un attaquant permet en effet de disposer de l'ensemble des privilèges sur le SI administré.

R32

Protéger l'accès aux annuaires des comptes d'administration

Il est fortement recommandé que le ou les annuaires contenant les comptes d'administration soient protégés en confidentialité et en intégrité et ne soient pas exposés sur des environnements de moindre confiance (ex. : SI bureautique).
Il est recommandé de déployer un annuaire dédié au SI d'administration en tant qu'infrastructure d'administration. Celui-ci gère les comptes d'administration et le contrôle d'accès aux ressources administrées.

Attention

Dans un environnement Windows, la migration des comptes d'administration depuis un Active Directory de production vers une nouvelle forêt (ou domaine) Active Directory d'administration est une opération complexe. Sa réalisation doit être accompagnée par des experts pour ne pas au final dégrader le niveau de sécurité du SI.

R33

Renforcer l'authentification pour les comptes d'administration

Il est fortement recommandé que l'opérateur s'assure que les comptes utilisés pour l'administration technique du SIE ne puissent être compromis en renforçant leurs mécanismes d'***authentification*** :

- utilisation de mots de passe complexes ;
- ***authentification à double facteur*** ;
- chiffrement ou hachage robuste [22] des secrets d'authentification, lorsqu'ils sont en transit ou stockés ;
- mécanismes de protection des mots de passe contre les attaques en ***force brute*** ;
- mécanismes de protection contre le rejeu de mots de passe.

Information

Au sujet du renforcement de l'authentification pour les comptes d'administration, le lecteur peut consulter le chapitre 7.2 du guide *Administration sécurisée des systèmes d'information* [27].

Un cas particulier de renforcement de l'authentification est le fait de ne pas garder de traces des secrets d'authentification, notamment dans les journaux.

R34

Empêcher le stockage des secrets d'authentification dans les journaux

L'opérateur doit configurer ses journaux de telle sorte qu'ils ne stockent aucune information sur les secrets utilisés pour l'authentification des comptes d'administration, que ce soit des éléments stockés en clair ou sous forme d'empreinte cryptographique.

Par ailleurs, il est nécessaire de limiter au strict nécessaire les actions d'administration permises à un administrateur : chacun de ses comptes d'administration doit uniquement disposer des droits relatifs aux actions dont ce compte est responsable, et uniquement sur le périmètre dont ce compte est responsable. C'est le ***principe du moindre privilège***.

Principe du moindre privilège

Principe qui énonce qu'une activité ne doit bénéficier que des autorisations strictement nécessaires à l'exécution des actions dont l'utilité est avérée.

22. La recommandation R32 du guide GNU/Linux [11] conseille « une fonction de hachage considérée comme sûre (SHA-256, SHA-512), avec un sel et un nombre de tours assez grand (65 536) ».

R35

⚖ Respecter le principe du moindre privilège dans l'attribution des droits d'administration

L'opérateur doit attribuer les droits d'administration aux comptes d'administration en respectant le principe du moindre privilège.

Exemple

Les droits d'accès attribués à un compte d'administrateur doivent refléter son domaine d'expertise technique (réseau, système, base de données, application, etc.) ou le périmètre fonctionnel qui lui est attribué (certains SI, certains équipements, certaines applications, etc.).
L'application de ce principe peut conduire à attribuer à un administrateur plusieurs comptes d'administration, chacun disposant de privilèges restreints sur des domaines ou périmètres précis.

4.3 Systèmes d'information d'administration (règle 12)

Les ressources matérielles et logicielles utilisées pour effectuer les actions d'administration constituent le ***SI d'administration***. Ce SI particulier doit être considéré comme très sensible.

Attention

Sans mesures de protection spécifiques, une compromission du SI d'administration a des conséquences majeures :

- l'attaquant a accès à tout ou partie des ressources d'administration, et contrôle alors les ressources administrées associées ;
- l'attaquant peut utiliser le SI d'administration pour contrôler les sources d'événement systèmes destinées à la journalisation, ou encore certains moyens de détection et de supervision, et réussir à masquer ses traces ; il est impossible de savoir exactement quelles ressources ont été compromises ;
- il devient obligatoire de reconstruire intégralement l'ensemble du système d'information, les comptes et le SI d'administration ne pouvant plus être considérés comme une base saine de reconstruction.

Objectif

S'assurer de l'intégrité des ressources utilisées pour réaliser les ***actions d'administration*** et de la confidentialité des informations que ces ressources manipulent, avec un niveau de confiance à la hauteur des enjeux pour le SIE administré.

En complément des segmentations logiques entre les actions d'administration et les autres actions, puis entre les comptes d'administration et les autres comptes, cette section recommande un cloisonnement fort, si possible physique, entre les ressources d'administration et les ressources administrées (dont le SIE et éventuellement d'autres ressources du SI d'entreprise de l'opérateur).

4.3.1 Maîtrise des ressources d'administration

Les ressources utilisées pour administrer le SIE sont des ressources critiques, dont le niveau de sécurité a un impact direct sur le niveau de sécurité du SIE.

Scénario d'attaque

L'opérateur fournit des postes de travail maîtrisés à ses administrateurs système. Cependant, pour faciliter ses astreintes, un administrateur a mis en place un accès au SIE depuis son ordinateur personnel, à son domicile.
Un attaquant envoie un courriel piégé à l'administrateur sur son adresse personnelle, et prend le contrôle de l'ordinateur personnel. Il y trouve les informations de connexion au SIE et peut à son tour accéder au SIE, à l'insu de l'administrateur.

L'opérateur doit avoir un haut niveau de confiance dans les équipements employés pour administrer le SIE. Toute pratique de type ***bring your own device (BYOD)***, non recommandée de manière générale, est à proscrire pour un poste d'administration.

R36

⚖ N'utiliser que des équipements maîtrisés pour l'administration

L'opérateur doit gérer et configurer les ressources matérielles et logicielles utilisées pour réaliser les ***actions d'administration***, ou les faire gérer et configurer par un prestataire mandaté pour réaliser ces actions.
En aucun cas l'utilisation d'un équipement personnel ne doit être tolérée pour l'administration d'un SI.

La gestion des équipements inclut notamment l'installation, le durcissement, le paramétrage, la personnalisation, la configuration des outils de sécurité, le maintien en conditions de sécurité, etc.

Toutes les ressources matérielles et logicielles des administrateurs doivent être gérées conformément à la politique de sécurité de l'opérateur. La règle 1 exige notamment que la PSSI définisse « les mesures de sécurité générales, notamment en matière de gestion et de sécurité des ressources […], d'exploitation et d'administration des SIE ».

4.3.2 Un système d'information dédié aux actions d'administration

Afin d'éviter la compromission de son SI d'administration, l'opérateur doit dédier ce SI aux actions d'administration, le cloisonner des ressources de moindre confiance, et filtrer les échanges avec ces ressources. Ces recommandations générales sont déclinées dans trois domaines :

- le poste de travail de l'administrateur ;
- le réseau utilisé pour se connecter aux ressources administrées ;
- les outils et serveurs de rebonds utilisés pour administrer les ressources.

La figure 4.1 illustre les composants d'un SI d'administration dédié aux actions d'administration.

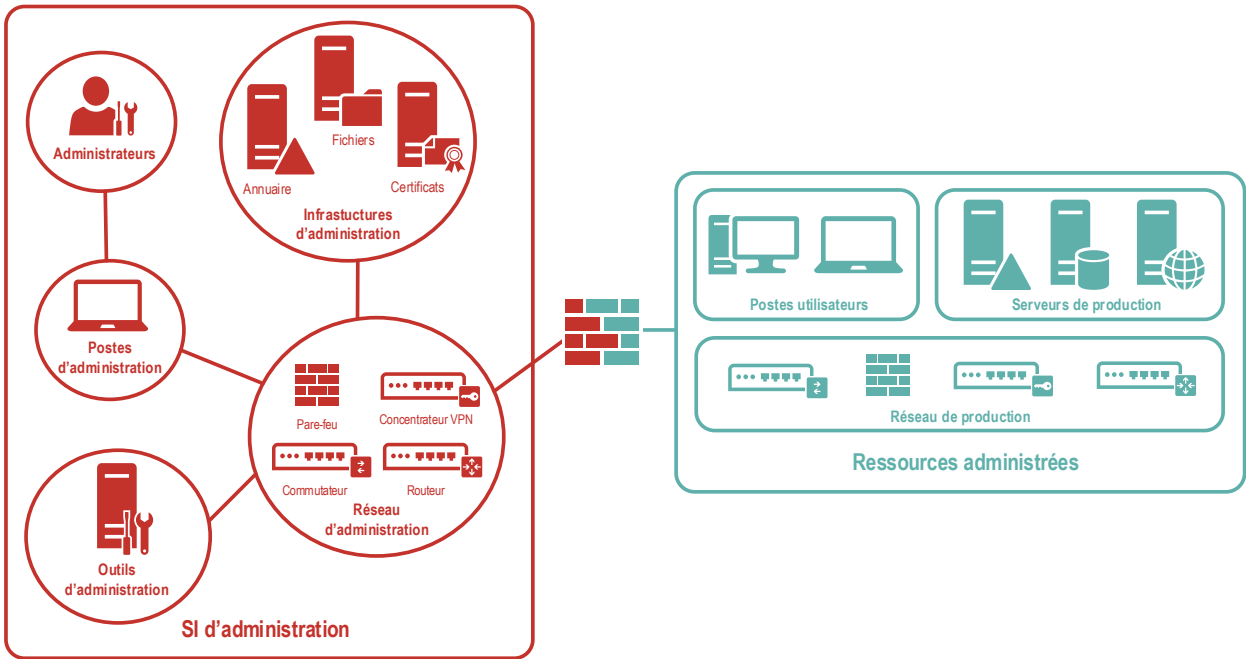

FIGURE 4.1 – Exemple d'un SI dédié aux actions d'administration

Information

Comme indiqué en préambule, le lecteur peut se référer aux publications de l'ANSSI :

- le guide *Administration sécurisée des systèmes d'information — v.2* [27] déjà cité, afin d'avoir une description des architectures possibles et des solutions techniques applicables ;
- le guide *La cybersécurité des systèmes industriels* [33], qui prend en compte les spécificités des systèmes industriels, et notamment son fascicule *Méthode de classification et mesures principales* [22] qui propose d'autres mesures de réduction du risque.

4.3.3 Poste d'administration

Un poste de travail usuel dispose de nombreuses applications (suite bureautique, navigateur, messagerie et autres outils de communication, applications métiers) ayant des niveaux de sécurité rarement évalués et souvent faibles. De plus, ce poste de travail échange avec des réseaux d'un faible niveau de confiance comme Internet. Ce poste de travail usuel a donc une surface d'attaque importante, et il est très exposé. Face à un attaquant motivé, ou simplement par la multiplication des attaques automatiques auxquelles ce poste est exposé, la compromission de ce poste est très probable.

Le poste de travail utilisé pour les actions d'administration sert à saisir et stocker de nombreux secrets liés aux SIE et à leur administration (identifiants, clés de chiffrement, fichiers de configuration, etc.). Ce poste est donc particulièrement sensible et doit être protégé en conséquence ; il est désigné ***poste d'administration***.

Scénario d'attaque

Un administrateur utilise un poste unique pour effectuer des actions d'administration et pour d'autres actions comme la navigation sur Internet ou la messagerie. Il respecte cependant la recommandation R29 et utilise des comptes distincts : un compte d'administration et un compte utilisateur.
Pendant une session ouverte en tant qu'utilisateur, il ouvre un courriel piégé et un attaquant prend le contrôle complet de son poste. Lorsque l'administrateur change de compte et ouvre une nouvelle session en tant qu'administrateur, l'attaquant capture le mot de passe du compte d'administration.

R37

⚖ Utiliser un poste d'administration dédié

L'opérateur doit dédier des postes de travail physiques à l'exécution aux actions d'administration.
Ce poste doit être distinct du poste permettant d'accéder aux autres ***environnements de travail*** usuels accessibles sur le SI de l'entité (ressources métier, messagerie interne, gestion documentaire, Internet, etc.).

Cette recommandation implique :

- qu'une action d'administration doit être effectuée depuis un poste physique dédié à l'administration ;
- que le poste d'administration ne peut être utilisé que pour les actions d'administration et aucune autre.

La figure 4.2 illustre une mise en œuvre de la recommandation R37 : l'administrateur dispose de deux postes, un premier en bleu pour son accès au SI bureautique et à Internet, et un second en rouge pour les actions d'administration.

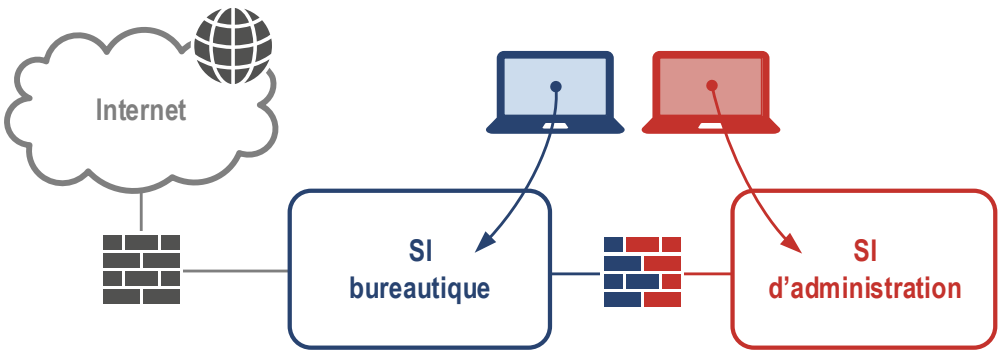

FIGURE 4.2 – Poste de travail dédié à l'administration

Cependant, lorsque des raisons techniques ou organisationnelles le justifient, la règle 12 prévoit que le poste de travail physique de l'administrateur peut être utilisé pour réaliser des actions autres que des actions d'administration. Dans ce cas, des mesures de réduction du risque doivent être prises.

Scénario d'attaque

Quelques exemples d'attaque visant des postes d'administration utilisés pour accéder à des ***environnements de travail*** usuels :

1. Un navigateur est utilisé à la fois pour naviguer sur Internet et pour se connecter à une console d'administration. Un greffon malveillant duplique les identifiants saisis et les envoie à l'attaquant.
2. Un poste de travail héberge deux machines virtuelles (VM), l'une pour naviguer sur Internet et l'autre pour effectuer des actions d'administration. Une vulnérabilité sur le logiciel de virtualisation permet de récupérer, depuis la VM de navigation, la mémoire de la VM d'administration (dont les mots de passe saisis) ou d'accéder aux fichiers disponibles dans la VM d'administration.
3. Un poste de travail est utilisé pour faire de la bureautique et pour se connecter à une machine virtuelle utilisée pour l'administration. L'utilisateur a téléchargé malgré lui un enregistreur de frappe (ou *keylogger*), et l'attaquant récupère les informations utilisées pour se connecter au SI d'administration (adresse de la machine, outils utilisés, identifiant et mot de passe, etc.).

R37 -

⚖ Accéder aux autres environnements de travail depuis le poste d'administration

Lorsque des raisons techniques ou organisationnelles le justifient, le poste de travail physique de l'administrateur peut être utilisé pour réaliser des actions autres que des actions d'administration.
L'opérateur doit mettre en place des mécanismes de durcissement et de cloisonnement pour isoler l'environnement logiciel utilisé pour ces autres opérations de l'environnement logiciel d'administration.

Information

Le chapitre 4.2 du guide *Administration sécurisée des systèmes d'information — v.2* [27] déjà cité détaille les configurations dérogatoires d'un niveau de sécurité moindre (R9 - pour un poste multi-niveau et R9 - - pour un accès à distance à la bureautique) et celles à proscrire pour les ***environnements de travail*** mixtes.

En particulier, l'architecture consistant à mettre en œuvre deux environnements de travail différents, virtualisés par un logiciel de virtualisation exécuté par un unique système d'exploitation, n'apporte pas un niveau de sécurité suffisant.

Il est également interdit de se connecter depuis un poste de travail de moindre confiance vers le SI d'administration, car toute compromission du poste de moindre confiance se propagerait au SI d'administration. Cela implique que tout élément technique utilisé pour se connecter doit être considéré comme faisant partie du système d'information d'administration.

Attention

La solution qui consiste à déployer un bastion comme moyen d'interconnexion depuis un poste d'un SI bureautique vers un SI d'administration est à proscrire. Elle procure un sentiment de sécurité injustifié puisqu'en réalité le bastion, porte d'entrée unique vers le SI d'administration, constitue une opportunité d'attaque importante, par exemple depuis un poste bureautique compromis depuis Internet.
Le chapitre 12.1 du guide *Administration sécurisée des systèmes d'information — v.2* [27] détaille les points d'attention à ce sujet.

Par ailleurs, le niveau de sécurité du poste d'administration doit être renforcé.

R38

⚖ Renforcer la sécurité du poste d'administration

L'opérateur doit renforcer la sécurité du poste d'administration.
Cela inclut notamment l'interdiction d'accès à Internet, le durcissement du système d'exploitation, la restriction des droits d'administration du poste pour l'utilisateur, la limitation des logiciels installés sur le poste, et l'utilisation de chiffrement pour les périphériques de stockage.

Information

Le chapitre 4.3 du guide *Administration sécurisée des systèmes d'information — v.2* [27] détaille les recommandations pour sécuriser le poste d'administration.

4.3.4 Réseau d'administration

Le réseau d'administration se définit comme le réseau de communication sur lequel transitent les flux internes au SI d'administration et les flux d'administration à destination des ressources administrées.

Comme le poste d'administration, le réseau d'administration est un élément clé de la sécurisation du SI d'administration. Le principe de cloisonnement doit conduire à le séparer des autres réseaux de sensibilité moindre.

Scénario d'attaque

Un opérateur met en œuvre un réseau mixte, utilisé pour les échanges métier et pour l'administration. Ce réseau est exposé indirectement à Internet.
Un attaquant réussit à compromettre un routeur de ce réseau et à créer une copie de tous les flux pour les rediriger vers sa machine. L'attaquant écoute l'ensemble du trafic (production, gestion, bureautique, etc.) dont les commandes d'administration. Il peut ainsi capter des fichiers ou des identifiants de connexion non chiffrés relatifs à l'administration.

À l'instar de la recommandation sur les postes d'administration, la mise en œuvre d'un *réseau d'administration* physiquement dédié aux ressources d'administration offre un niveau de sécurité maximal pour se prémunir d'une compromission du SI d'administration et garantir un cloisonnement fort avec tout autre réseau potentiellement connecté à Internet.

Pour éviter le branchement d'équipements indésirables sur ce réseau d'administration dédié (postes bureautiques, postes personnels), une authentification réseau est recommandée en complément, par exemple par l'implémentation du protocole 802.1x [13].

R39

⚖ Connecter les ressources d'administration sur un réseau physique dédié

L'opérateur doit déployer les ressources d'administration (ex. : postes d'administration, serveurs outils) sur un réseau physiquement dédié à cet usage.
Afin de renforcer le contrôle d'accès au réseau d'administration, il est recommandé que les postes d'administration s'authentifient lorsqu'ils se connectent à ce réseau.

Information

Les réseaux Wi-Fi sont par nature des réseaux partagés. Ils ne peuvent être considérés comme des réseaux physiquement dédiés à l'administration, ni même comme des réseaux maîtrisés. Les recommandations citées dans le cadre des accès à distance s'appliquent, dont la recommandation R22.

Si l'application stricte de cette recommandation est techniquement impossible (par exemple sur un réseau étendu), une alternative d'un niveau de sécurité moindre peut être envisagée sur la base d'un cloisonnement par le chiffre.

R39 -

⚖ Connecter les ressources d'administration sur un réseau VPN IPsec dédié

Lorsque l'opérateur ne peut dédier un réseau physique à l'administration et que, pour des raisons techniques, les flux d'administration circulent sur d'autres réseaux, l'opérateur doit déployer les ressources d'administration sur un réseau logique dédié à cet usage en mettant en œuvre des mécanismes de chiffrement et d'authentification de réseau, à savoir le protocole IPsec.
En complément, des mécanismes de segmentation logique (VLAN) et de filtrage réseau sont recommandés pour limiter l'exposition du concentrateur VPN IPsec aux seuls postes d'administration.
Pour la mise en œuvre du protocole IPsec, les recommandations du guide de l'ANSSI [24] doivent être appliquées.

Exemple

L'opérateur peut avoir besoin d'un réseau à usage mixte lorsqu'il est sur un système isolé avec un réseau unique (donc sans possibilité de dédier physiquement un réseau) ou dans le cas d'une télé-administration depuis un autre site, voire au travers d'un réseau public comme Internet. Dans ce dernier cas, les recommandations de la section 3.3 s'appliquent également.

R39 - -

⚖ Pallier l'absence de chiffrement des flux d'administration

Lorsque des raisons techniques empêchent de chiffrer et d'authentifier les flux d'administration lorsqu'ils circulent sur d'autres réseaux, l'opérateur doit mettre en œuvre des mesures permettant de protéger la confidentialité et l'intégrité de ces flux et de renforcer le contrôle et la traçabilité des opérations d'administration.
L'opérateur doit décrire les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.

Parmi les mesures de réduction du risque possibles, on peut citer le contrôle d'accès logique ou physique au réseau transportant les flux en clair, et une supervision renforcée des accès et des opérations d'administration.

Par ailleurs, l'accès aux ressources administrées doit être maîtrisé, non seulement au niveau réseau par des mesures de blocage et de filtrage, mais aussi au niveau local grâce à des configurations applicatives sur ces ressources.

Ainsi, la recommandation R23+ relative au filtrage local s'applique en particulier aux flux d'administration vers les ressources administrées : seules des ressources d'administration identifiées doivent pouvoir accéder aux services d'administration. Par exemple, le service de production d'un serveur Web est accessible sur le port TCP/443 (HTTPS) par l'ensemble des clients légitimes, alors que son service d'administration est accessible sur le port TCP/22 (SSH) uniquement par les ressources d'administration gérant ce serveur.

Information

Certains systèmes, par exemple des systèmes de gestion de contenu ou le service Active Directory de Microsoft, ne distinguent pas le port d'écoute des services de production et d'administration (même port TCP). Dans ce cas de figure, l'application de R23+ est toujours nécessaire mais non suffisante.
La sécurité de l'administration au niveau de la ressource administrée repose de façon ultime sur la configuration applicative du service (ex. : contrôle d'accès, gestion des droits) et sa robustesse ; cela doit être traité avec attention mais n'est pas l'objet de ce guide.

Dès lors qu'elle est techniquement réalisable au niveau d'une ressource administrée, la séparation des interfaces de production et d'administration est recommandée. Cette mesure garantit non seulement un filtrage local plus spécifique (ex. : un service d'administration n'est accessible qu'à travers l'interface d'administration) mais aussi une disponibilité accrue de la ressource administrée en cas de déni de service sur le réseau de production.

Une séparation en interfaces réseau physiques offre un niveau de sécurité maximal et permet ainsi de dissocier les équipements de filtrage réseau respectivement sur les réseaux de production et d'administration. À défaut, une séparation en interfaces réseau virtuelles est recommandée.

Si cette séparation n'est techniquement pas réalisable sur un système, alors l'application des mesures locales, dont la recommandation R23+, doit être d'autant plus stricte.

R40

Dédier une interface réseau physique d'administration

Il est recommandé de dédier une interface réseau physique d'administration sur les ressources administrées en s'assurant des prérequis suivants :

- les services logiques permettant l'exécution des actions d'administration doivent être en écoute uniquement sur l'interface réseau d'administration prévue à cet effet ;
- les fonctions internes du système d'exploitation ne doivent pas permettre le routage d'informations entre les interfaces réseau de production et l'interface réseau d'administration d'une même ressource. Elles doivent être désactivées (ex. : désactivation d'*IP Forwarding*).

R40 -

Dédier une interface réseau virtuelle d'administration

À défaut d'une interface réseau physique d'administration, il est recommandé de dédier une interface réseau virtuelle d'administration sur les ressources administrées. Les mêmes prérequis que R40 s'appliquent.

Une illustration d'un réseau mixte est donnée dans la figure 4.3. Parmi les trois groupes de ressources administrées représentés à droite de la figure, celui du haut dispose d'un réseau physique dédié à l'administration ; le groupe du milieu dispose d'interfaces logiques dédiées à l'administration, accédé à travers un réseau mixte ; et le groupe du bas ne dispose pas d'interfaces d'administration et il est accédé à travers le réseau mixte.

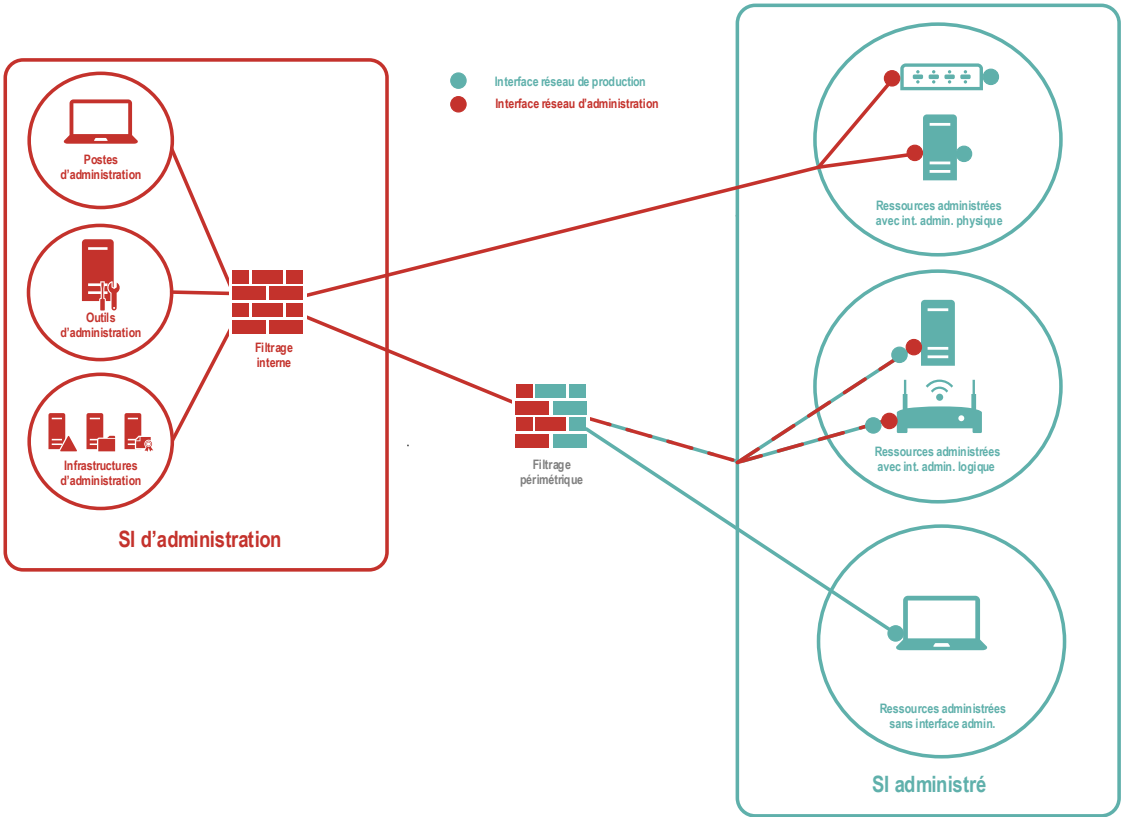

FIGURE 4.3 – Réseau dédié à l'administration jusqu'aux interfaces des machines

Enfin, les principes de cloisonnement et de filtrage décrits dans les sections 3.2 et 3.4 doivent être appliqués au SI et au réseau d'administration.

R41

Cloisonner et filtrer le réseau d'administration

Il est fortement recommandé de cloisonner et de filtrer le réseau d'administration, avec en particulier :

- un filtrage interne au sein du SI d'administration, entre zones de confiance (postes d'administration, serveurs d'infrastructures, outils, les différents réseaux de ressources administrées) ;
- un filtrage périmétrique à toutes les interconnexions du SI d'administration avec d'autres SI ;
- un filtrage local sur chaque ressource administrée ;
- l'activation du PVLAN sur les commutateurs reliant les ressources administrées, pour interdire les flux entre ressources administrées à travers le réseau d'administration.

Information

Ces mesures sont détaillées dans le chapitre 5 du guide *Administration sécurisée des systèmes d'information – v2.0* [27].

4.3.5 Protocoles d'administration

Les protocoles utilisés pour administrer le SIE contribuent eux aussi à la sécurité des flux d'administration. Le recours aux versions chiffrées de ces protocoles, lorsqu'elles existent, protège l'intégrité et la confidentialité des informations relatives à l'administration.

R42

Utiliser des protocoles sécurisés pour l'administration

Les flux d'administration étant particulièrement sensibles, il est fortement recommandé que l'opérateur utilise une version sécurisée des protocoles d'administration permettant de protéger la confidentialité et l'intégrité de ces flux.
Le cas échéant, les protocoles non sécurisés doivent être explicitement désactivés ou bloqués.

4.3.6 Administration de plusieurs SI

Le SI d'administration utilisé pour le SIE peut aussi servir à administrer d'autres SI. Pour rappel, un poste d'administration peut disposer d'outils installés localement ou, de manière non exclusive, accéder à des serveurs outils d'administration.

Un administrateur peut disposer d'un poste unique pour l'administration de différentes zones de confiance (par exemple, un SIE et d'autres SI), aux conditions suivantes :

- la sécurisation du poste d'administration doit être en phase avec les besoins de sécurité de la zone de confiance administrée la plus exigeante ;

- les serveurs outils accessibles depuis le poste d'administration ne doivent pas être mutualisés pour l'administration de deux zones de confiance distinctes (en d'autres termes, un serveur outils reste dédié à une unique zone de confiance et est cloisonné – voir section 3.2) ;
- les éventuels outils installés sur le poste d'administration ne doivent pas permettre un rebond entre deux ressources administrées de deux zones de confiance distinctes ;
- l'accès aux différentes zones de confiance depuis le SI d'administration doit respecter le cloisonnement, physique ou logique, entre zones de confiance (en d'autres termes, deux pare-feux physiques ou un pare-feu configuré avec deux DMZ sont déployés en périphérie du SI d'administration, pour respecter le cloisonnement des zones de confiance).

Les figures 4.4 et 4.5 représentent les cas de mutualisation d'un poste d'administration de deux zones de confiance distinctes, respectivement d'un niveau de confiance homogène (par exemple deux SIE) ou hétérogène (un SIE et le SI bureautique).

R43

Administrer des SI différents avec des serveurs outils différents

L'opérateur souhaitant administrer deux SI différents (un SIE et un autre SI par exemple) peut le faire depuis le même SI d'administration si celui-ci respecte les recommandations du présent chapitre.
Il est alors recommandé que l'opérateur dédie un serveur outils à l'administration du SIE et respecte le cloisonnement, physique ou logique, entre zones de confiance jusque dans la zone des serveurs outils.

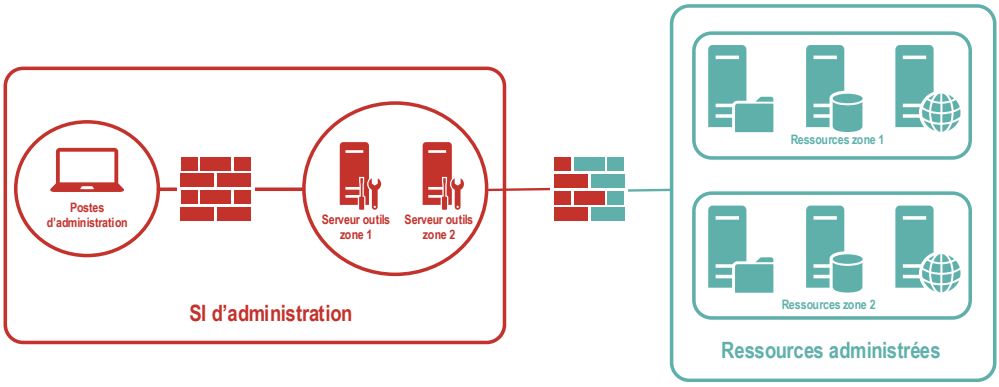

FIGURE 4.4 – Mutualisation du poste d'administration pour deux zones de confiance homogène

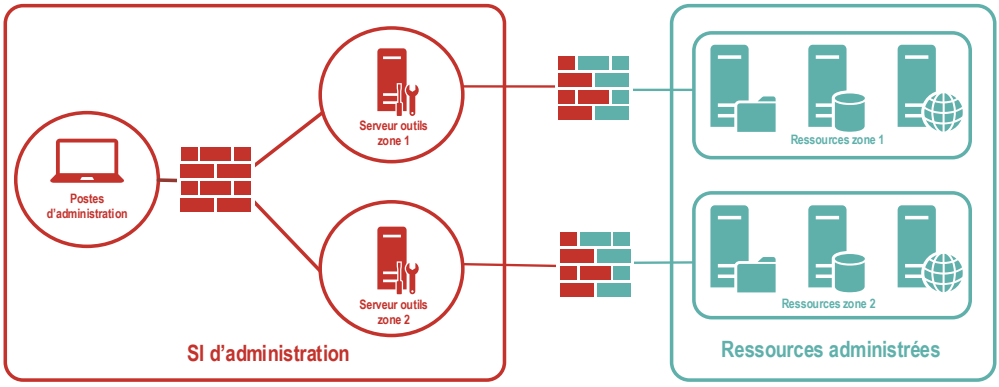

FIGURE 4.5 – Mutualisation du poste d'administration pour deux zones de confiance hétérogène

5
Gestion des identités et des accès (règles 13 à 15)

Ce chapitre détaille les recommandations relatives à la section 3 du chapitre II de l'*arrêté du 14 septembre 2018*. Il couvre les règles relatives à l'identification (règle 13), à l'authentification (règle 14), et à la gestion des droits d'accès (règle 15), respectivement dans les sections 5.1, 5.2 et 5.3.

5.1 Identification (règle 13)

Objectif

Pouvoir attribuer toute action effectuée sur un SI à un utilisateur ou à un processus automatique, en associant une identité à chaque personne ou processus, puis une identité à chaque action effectuée.

Identification

Action d'un utilisateur ou d'un processus automatique consistant à communiquer une identité préalablement enregistrée.

Imputabilité

Capacité d'attribuer une action de façon certaine à un utilisateur ou à un processus automatique.

5.1.1 Utilisation de comptes individuels

Scénario d'attaque

Dans un SIE, un compte nommé « Utilisateur » sert à se connecter à une application sensible. Ce compte est utilisé par quinze personnes qui appartiennent à la même équipe.
À la suite d'un incident, une investigation amène à retrouver dans les journaux de l'application que le compte « Utilisateur » a effectué il y a quatre mois une action en lien avec l'incident. Il est cependant impossible de savoir exactement quelle personne de l'équipe a réalisé cette action. Cela laisse aussi le doute sur la possibilité qu'un attaquant utilise aussi le compte à l'insu de l'équipe.

Un ***compte individuel*** correspond :

- soit à un seul utilisateur (personne physique), identifiable par son nom ou par un identifiant unique ;
- soit à un ***compte technique*** rattaché à un processus automatique (un programme, une application, un service, un script, etc.). Un ***compte technique*** ne doit pas pouvoir ouvrir une session interactive [23].

R44

⚖ Utiliser des comptes individuels

L'opérateur doit attribuer un ***compte individuel*** à chaque utilisateur ou processus automatique qui accède au SIE ou l'utilise.

Information

La recommandation R44 n'est pas applicable lorsqu'un service essentiel nécessite de diffuser de l'information au public ; l'opérateur n'est pas tenu de créer des ***comptes individuels*** pour l'accès du public à cette information.

À l'inverse, un ***compte partagé*** est commun à plusieurs personnes ou à plusieurs processus automatiques. En conséquence, l'utilisation de ***comptes partagés*** ne permet plus d'associer de façon unique un compte et une personne ou un processus automatique.

Exemple

Des cas particuliers peuvent imposer la création de comptes partagés. Cela empêche cependant la stricte imputabilité de chaque opération effectuée et est donc contraire à ce qui est exigé dans la recommandation R44. Par exemple :

- les équipements n'offrant pas de mécanisme technique de gestion de comptes et n'utilisant qu'un seul compte, voire pas de compte du tout. Ils ne permettent donc pas de créer un compte pour chaque utilisateur ;
- les équipements qui doivent maintenir dans la durée une même session active (leurs activités sont interrompues par la fermeture de la session). Dans ce cas, les utilisateurs ne peuvent pas recourir à des sessions différentes, ouvertes avec leurs comptes individuels respectifs. C'est le cas sur des systèmes industriels dont le temps d'opération peut être plus long que la présence d'un utilisateur unique ;
- certaines activités nécessitent l'utilisation par plusieurs utilisateurs d'une session unique, simultanément ou séquentiellement, pour des raisons organisationnelles. Cela peut être le cas de personnes chargées d'accueil du public dans un bâtiment, de personnes entrant des données dans un laboratoire, etc.

Dans tous ces cas particuliers où l'imputabilité d'une action à un utilisateur unique n'est plus assurée par l'utilisation d'un compte individuel, l'opérateur met en place des mesures techniques ou organisationnelles permettant d'atteindre un niveau d'imputabilité équivalent.

23. Pour les comptes techniques dans les environnements Linux, voir les recommandations R27 et R28 des *recommandations de configuration d'un système GNU/Linux* [11], ou encore la recommandation R24 des *recommandations pour un usage sécurisé d'(Open)SSH* [9].

R44 -

⚖ Pallier l'absence de comptes individuels

Lorsque des raisons techniques ou opérationnelles empêchent de créer des comptes individuels pour les utilisateurs ou pour les processus automatiques, l'opérateur doit mettre en place des mesures pour réduire le risque lié à l'utilisation de comptes partagés. Les objectifs sont d'assurer la traçabilité de l'usage de ces comptes et d'en détecter les usages malveillants.
L'opérateur doit décrire les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.

Exemple

Pour réduire le risque associé à un compte partagé, il est possible de limiter :
- la plage horaire pendant laquelle le compte peut ouvrir une session ;
- les équipements pouvant utiliser ces comptes ;
- l'accès physique à ces équipements.

Pour assurer la traçabilité de l'utilisation d'un compte partagé, il est possible :
- d'utiliser un cahier d'enregistrement décrivant précisément la date et l'heure de présence du personnel à un poste d'astreinte particulier ;
- d'utiliser un bastion assurant la traçabilité entre une identité individuelle et le recours à un compte partagé ;
- sur un système Unix, d'utiliser la commande `sudo` qui permet de savoir quel utilisateur a fait usage du compte `root` en consultant les journaux du système.

La journalisation et la supervision des accès et des actions des comptes partagés contribuent à la détection des incidents de sécurité.

5.1.2 Comptes inutilisés

La protection des comptes des utilisateurs passe aussi par leur désactivation dès lors qu'ils ne sont plus utilisés.

Scénario d'attaque

Un utilisateur ayant un compte actif sur le SIE part à la retraite et son compte reste actif.
Comme plus personne n'utilise ce compte, un attaquant a plus de temps pour découvrir son secret d'authentification et obtenir un accès à ce compte, et il a toute latitude pour l'utiliser sans être détecté par son détenteur légitime.

R45

⚖ Désactiver les comptes inutilisés

L'opérateur doit désactiver sans délai les comptes individuels ou partagés qui ne sont plus nécessaires.

La désactivation d'un compte revient à la suspension globale des droits d'accès qui lui étaient attribués, voire à leur suppression. Cette désactivation doit être systématique pour tout compte qui n'a plus vocation à être utilisé.

La simple désactivation d'un compte est parfois préférable à la suppression complète du compte, pour permettre de conserver la traçabilité des actions dans le temps, ou pour conserver des données liées au compte de l'utilisateur (clés de chiffrement, certificats, etc.). Dans ce cas, il est recommandé que l'opérateur désactive *complètement* le compte. Il peut pour cela appliquer des mesures techniques supplémentaires : modification du mot de passe par un nouveau mot de passe aléatoire, interdiction d'ouverture de session, suppression des droits et privilèges [24], déplacement dans une unité organisationnelle d'annuaire dédiée, etc.

La désactivation du compte peut aussi se faire en cas d'absence prolongée de la personne titulaire du compte : congé sabbatique, congé parental, congé maladie, etc. Le compte est alors réactivé au retour de son titulaire.

Cette recommandation est aussi valable pour les comptes créés par défaut lors de l'installation d'un système et qui n'ont pas vocation à être utilisés ensuite, comme évoqué dans la section 3.1.1.1.

Enfin, cette recommandation s'applique également aux comptes inutilisés depuis un certain temps (par exemple un an).

5.1.3 Revues de comptes

Afin que ces recommandations soient efficaces, l'opérateur peut utiliser des outils d'audit automatiques en lien avec son annuaire. Il doit aussi faire régulièrement des revues afin d'avoir une visibilité sur les comptes présents sur le SIE. Il est recommandé de lier cette revue des comptes actifs avec une revue des droits d'accès, évoquée par la recommandation R57.

5.2 Authentification (règle 14)

Objectif

Vérifier l'identité d'une personne physique ou d'un processus automatique avant de lui donner accès au SIE.

Authentification

Processus ayant pour but de vérifier l'identité dont se réclame un utilisateur, un processus, une entité ou une machine.
S'authentifier consiste à apporter la preuve de cette identité au moyen d'un ou plusieurs ***facteurs d'authentification***. L'authentification est donc précédée d'une ***identification***.

24. Si les droits sont attribués à des groupes conformément à la recommandation R55, le compte désactivé ne doit plus être membre de ces groupes.

Information

Lorsqu'un service essentiel nécessite de diffuser de l'information au public, l'opérateur n'est pas tenu de mettre en place des mécanismes d'authentification pour l'accès du public à cette information.

5.2.1 Secret d'authentification

L'accès à une ressource d'un SIE doit être conditionné à la connaissance ou à la possession d'un secret (mot de passe, code PIN, clé privée, etc.).

Scénario d'attaque

Il est possible d'ouvrir une session interactive sur une machine sans authentification. Un attaquant ayant déjà accès au réseau se connecte à la machine, et peut exécuter toutes les actions permises au compte actif dans cette session.

5.2.1.1 Sécurité du mécanisme d'authentification

R46

⚖ Mettre en œuvre un mécanisme d'authentification pour chaque compte

L'opérateur doit protéger les accès aux ressources de ses SIE, que ce soit par un utilisateur ou par un processus automatique, au moyen d'un mécanisme d'authentification impliquant au minimum un élément secret.

Cette authentification peut être renforcée par l'emploi d'une ***authentification à double facteur*** s'appuyant sur plusieurs types de ***facteurs d'authentification***.

Le secret qui est utilisé dans le mécanisme d'authentification est un des moyens de s'assurer que l'utilisateur ou le processus automatique est bien celui qu'il prétend être : la compromission d'un secret peut conduire à ce qu'un attaquant utilise frauduleusement un compte. La confidentialité et l'intégrité des secrets doivent donc être particulièrement protégées.

R47

⚖ Établir une politique de gestion des secrets d'authentification

L'opérateur doit définir et appliquer une politique de gestion des éléments secrets d'authentification, dont les mots de passe, en accord avec sa politique de sécurité des systèmes d'information.
En particulier, l'opérateur doit configurer le SIE pour forcer le choix de mots de passe conformes à cette politique (longueur, types de caractères, fréquence de renouvellement).

Cette politique de gestion doit décrire les éléments secrets utilisés et les mécanismes de sécurité mis en œuvre pour les protéger.

Les mots de passe ne doivent pas être stockés en clair (en dehors des cas de séquestre dans un coffre-fort). Suivant les contextes, il est préconisé de ne stocker que des mots de passe chiffrés

ou que le résultat obtenu en appliquant un algorithme de dérivation de clef dédié à cette usage (comme ARGON2 ou PBKDF2) au mot de passe et à un sel. L'utilisation d'algorithmes réversibles ou de simple empreintes sont à proscrire.

Les mots de passe doivent être conformes à l'état de l'art tel que défini par l'ANSSI en matière de complexité (longueur du mot de passe et types de caractères) et de renouvellement, en tenant compte du niveau de complexité maximal permis par la ressource concernée.

Information

Le lecteur peut se reporter aux documents suivants pour la définition de l'état de l'art pour la gestion des mots de passe :

- le guide *Authentification par mot de passe - les mesures de sécurité élémentaires* [25] de la CNIL ;
- l'outil de calcul de la force d'un mot de passe présent sur le site de l'ANSSI [26] ;
- la note technique *Recommandations de sécurité relatives aux mots de passe* de l'ANSSI [8] ;
- le *Guide d'hygiène informatique* de l'ANSSI [16].

L'opérateur doit faire appliquer les règles automatiquement dans les outils de saisie et de modification de mots de passe, de sorte qu'il ne soit pas possible de créer ou de changer un mot de passe sans qu'il soit conforme à ces règles.

5.2.1.2 Partage de secrets

Si un élément secret d'authentification venait à être connu de personnes n'ayant pas ou plus le besoin de le connaître, alors l'élément ne peut plus être considéré comme étant secret. L'imputabilité n'est plus garantie.

R48

⚖ Interdire le partage de secrets d'authentification

L'opérateur doit interdire le partage d'éléments secrets entre plusieurs utilisateurs et sensibiliser ses utilisateurs sur le fait qu'un secret d'authentification ne doit pas être divulgué.

Ainsi, il est proscrit d'inscrire en clair un mot de passe sur un support accessible à d'autres personnes que celles qui ont besoin de connaître ce mot de passe.

R48 -

⚖ Protéger les secrets d'authentification des comptes partagés

Dans le cas d'un compte partagé, le partage du secret d'authentification ne doit se faire strictement qu'entre les personnes ayant le besoin d'utiliser le compte partagé. Cela implique en particulier que le secret associé à un compte partagé doit être renouvelé chaque fois qu'un utilisateur perd le besoin métier légitime d'utiliser ce compte, ou que la confidentialité du mot de passe n'est plus assurée.

25. https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires
26. https://www.ssi.gouv.fr/administration/precautions-elementaires/calculer-la-force-dun-mot-de-passe

5.2.2 Renforcement de l'authentification

Certains cas nécessitent d'utiliser une authentification renforcée afin de s'assurer, avec un haut niveau de confiance, de l'identité de l'utilisateur.

5.2.2.1 Cas des comptes privilégiés

Compte privilégié

Compte dont les droits d'accès permettent des actions qui ne sont pas autorisées à la majorité des utilisateurs de l'application ou du SI.
C'est par exemple le cas d'un compte d'administrateur technique. Cela peut être aussi le cas d'un compte d'administrateur métier qui permet de définir les droits des autres utilisateurs dans une application.
Il existe également des comptes de processus ou de service avec des privilèges élevés. Ces comptes sont des comptes privilégiés sans être des comptes d'administration.

R49

Dédier un mot de passe à chaque compte privilégié

Lorsque les éléments secrets d'authentification sont des mots de passe, les utilisateurs ne doivent pas les réutiliser entre plusieurs comptes, privilégiés ou non privilégiés.
Il est fortement recommandé que le mot de passe d'un compte privilégié ne puisse pas être déduit d'un mot de passe d'un autre compte du même utilisateur.

La bonne mise en œuvre de la recommandation R49 ne peut pas être vérifiée par un dispositif technique [27]. Cette recommandation est donc avant tout organisationnelle et passe par la formation des utilisateurs et administrateurs.

Certains utilisateurs, et notamment les administrateurs, peuvent être amenés à utiliser un nombre important de secrets, ce qui rend le respect des bonnes pratiques difficile à maintenir dans le temps. Le stockage des mots de passe dans un fichier, en clair ou avec un chiffrement faible, doit être proscrit. L'utilisation d'un coffre-fort de mots de passe est recommandée notamment dans ce cas.

R50

Stocker les mots de passe dans un coffre-fort de mots de passe

Il est recommandé d'utiliser un coffre-fort de mots de passe pour stocker de manière sécurisée les mots de passe, en particulier pour les comptes privilégiés. Il est recommandé de privilégier les solutions disposant d'un visa de sécurité de l'ANSSI.

27. Sauf à stocker les mots de passe en clair, ce qui serait incompatible avec la nature secrète de ces éléments d'authentification.

5.2.3 Renouvellement des secrets

5.2.3.1 Renouvellement régulier des secrets

Les secrets d'authentification ont une grande valeur pour les attaquants, qui disposent de nombreux outils pour automatiser la recherche de ces informations. Face à cette menace, il est imprudent de considérer qu'un secret d'authentification peut être utilisé indéfiniment. En effet :

- au cours de l'exploitation d'un SI, de plus en plus de personnes sont amenées à s'y connecter et donc à connaître des secrets d'authentification ;
- plus la période de renouvellement d'un secret est longue, plus un attaquant a de temps pour découvrir ce secret.

Scénario d'attaque

L'opérateur n'a pas de politique de renouvellement des mots de passe du SIE.
Un attaquant a réussi à récupérer une base de mots de passe hachés associée au SIE.
L'attaquant utilise des outils d'attaque en ***force brute*** et obtient des mots de passe en clair [28]. Une fois les mots de passe obtenus, l'attaquant peut s'en servir indéfiniment pour contrôler des comptes sur le SIE.

R51

⚖ Renouveler régulièrement les secrets d'authentification

L'opérateur doit renouveler régulièrement les secrets d'authentification.
La fréquence de renouvellement doit être choisie en accord avec la PSSI et doit répondre à l'objectif de protection des SIE concernés.

R51 -

⚖ Pallier l'impossibilité de modifier un secret d'authentification

Lorsque la ressource ne permet pas techniquement de modifier l'élément secret d'authentification, l'opérateur doit mettre en place des mesures techniques et organisationnelles permettant de réduire les risques associés à ce secret fixe.
L'opérateur doit décrire les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.
Ces mesures concernent en particulier le contrôle d'accès physique à la ressource concernée ou la traçabilité (horaire, durée, etc.) des accès, afin de rattacher indirectement une action à une personne.

Il convient de compléter cette approche par une protection de la méthode de renouvellement du secret, afin que le nouveau secret employé ne soit pas directement à la disposition de l'attaquant.

28. D'autres d'attaques comme *pass-the-hash* s'appuient non pas sur le recouvrement des mots de passe en clair mais sur la réutilisation des mots de passe hachés, quand le protocole d'authentification y est vulnérable (comme NTLM).

R52

⚖ Contrôler le renouvellement et l'accès aux secrets d'authentification

L'opérateur doit s'assurer que seuls les utilisateurs qui en ont la responsabilité peuvent modifier les éléments secrets d'authentification et peuvent accéder, si nécessaire, à ces secrets en clair.

La possibilité de modifier un élément d'authentification d'un compte ne doit être accessible qu'aux personnes ayant légitimement ce rôle, comme l'utilisateur du compte, un administrateur, ou une personne chargée du support utilisateur.

Lorsqu'un mot de passe est modifié par une autre personne que l'utilisateur lui-même, alors l'utilisateur doit à nouveau changer le mot de passe lors de sa première connexion.

5.2.3.2 Renouvellement ponctuel des secrets

En plus du renouvellement régulier, certains cas particuliers demandent une modification ponctuelle et parfois immédiate des secrets d'authentification, en particulier des mots de passe :

- lorsque ce sont des éléments définis par défaut (cf. R1) ;
- lorsqu'il s'agit d'un compte partagé et qu'une personne connaissant ce secret partagé n'en a plus besoin (cf. R48-) ;
- lors de la première authentification après attribution d'un mot de passe temporaire à un compte d'utilisateur ;
- lorsqu'il y a une suspicion de compromission ou une compromission avérée.

R53

Renouveler immédiatement des secrets d'authentification

Lorsque les conditions de sécurité protégeant un secret d'authentification ne sont plus réunies, il est fortement recommandé que l'opérateur renouvelle immédiatement ce secret.

5.3 Droits d'accès (règle 15)

Objectif

S'assurer que les utilisateurs ont uniquement accès aux ressources et aux fonctions qui leur sont légitimement nécessaires.

Scénario d'attaque

Un SIE ne met pas en œuvre de gestion des droits des utilisateurs : il existe un seul type ou profil d'utilisateur, doté de tous les droits.
Un attaquant a compromis un compte utilisateur légitime, dont le mot de passe était faible. L'attaquant a maintenant accès à l'ensemble des fonctions du SIE, y compris celles dont le compte compromis n'avait pas besoin.

5.3.1 Attribution des droits d'accès

R54

⚖ Définir une politique de gestion des droits d'accès

L'opérateur doit définir les règles de gestion et d'attribution des droits d'accès aux ressources de ses SIE, conformément à sa politique de sécurité des systèmes d'information.

Cette politique doit préciser formellement la façon dont les droits d'accès aux SIE sont attribués et maintenus dans le temps :

- définition de rôles métier et de profils techniques standards ;
- cycle de vie des droits : modalités d'attribution, de modification et de suppression de droits ;
- outillage technique associé ;
- modalités de contrôle ;
- etc.

Il est recommandé de recourir à une méthodologie définissant des rôles et des profils (par exemple suivant la méthodologie ***RBAC***), pour que l'attribution de droits d'accès soit systématique et non redéfinie manuellement au cas par cas, ce qui est souvent source d'erreur. Dans un annuaire, les rôles et profils sont souvent représentés par des groupes de comptes.

R55

⚖ Attribuer les droits d'accès suivant le principe du moindre privilège

L'opérateur doit n'attribuer à un utilisateur ou à un processus automatique que les droits strictement nécessaires à l'exécution des actions dont l'utilité est avérée.
Il est recommandé qu'aucun droit ne soit attribué par défaut à un utilisateur ou à un processus automatique.
Il est recommandé que les droits soient attribués à groupes de comptes.

Le principe du moindre privilège implique de limiter le niveau de droits qu'on attribue sur une ressource, mais aussi de ne donner accès qu'aux fonctions de cette ressource qui sont nécessaires. L'opérateur doit déterminer quels sont les droits d'accès unitaires disponibles sur une ressource (système, application, etc.), puis déterminer comment ces droits unitaires sont attribués à un compte donné ou à un groupe de comptes donné (comme recommandé notamment pour les groupes d'administrateurs par R31).

Attention

Lors d'un changement de fonctions au sein de l'opérateur, un utilisateur doit donc perdre les droits associés à ses anciens rôles et profils et se voir attribuer les droits associés à ses nouvelles fonctions. L'opérateur peut mettre en place une période de recouvrement afin de s'assurer que l'utilisateur a bien tous les droits nécessaires pour une période de transition. Cependant, cette période doit être limitée dans le temps.

Un cas particulier de l'attribution détaillée de droits d'accès concerne les ***comptes privilégiés***, notamment les ***comptes d'administration***. Ces comptes sont particulièrement sensibles et nécessitent une traçabilité particulière.

R56

⚖ Définir une traçabilité des comptes privilégiés

L'opérateur doit établir et tenir à jour la liste des comptes privilégiés.
Toute modification d'un compte privilégié (ajout, suppression, suspension ou modification des droits associés) doit faire l'objet d'un contrôle formel de l'opérateur destiné à vérifier que les droits d'accès aux ressources et fonctionnalités sont attribués selon le principe du moindre privilège et en cohérence avec les besoins du compte.

La liste des comptes privilégiés doit faire partie de la cartographie globale du SIE exigée par la règle 6. La liste doit préciser, pour chaque compte, le niveau et le périmètre des droits d'accès associés, ainsi que les types de comptes sur lesquels portent ces droits (comptes d'utilisateurs, comptes de messagerie, comptes de processus, etc.).

Cette liste doit être à jour, ce qui implique que chaque modification concernant un compte privilégié doit être tracée et validée par l'opérateur. Enfin, il est important que la gestion des comptes privilégiés soit systématiquement intégrée aux processus d'arrivée, de départ ou de gestion interne du personnel (mutations, congés, etc.).

Concernant le contrôle formel des modifications des comptes privilégiés, il est recommandé qu'il soit fait par deux personnes, l'une ayant les connaissances métier suffisantes pour s'assurer que l'utilisateur est bien légitime et l'autre connaissant bien le fonctionnement technique de la ressource concernée.

5.3.2 Revue des droits d'accès

De nombreuses attaques sont facilitées par le fait que des droits d'accès qui ont été attribués à un utilisateur (ou à un administrateur) ne suivent pas forcément l'évolution de la situation de cet utilisateur dans le temps. Ainsi, des droits attribués peuvent ne plus correspondre au strict besoin de l'utilisateur quelques mois ou quelques années plus tard.

R57

⚖ Faire une revue régulière des droits d'accès

L'opérateur doit faire une revue régulière des droits d'accès attribués, au moins tous les ans. Cette revue est également une opportunité pour détecter des comptes à désactiver.
Cette révision porte sur les liens entre les comptes, les droits d'accès associés et les ressources ou les fonctionnalités qui en font l'objet.

Cette revue des droits d'accès attribués aux utilisateurs et aux processus automatiques permet de s'assurer de l'efficacité de la procédure d'attribution de droits dans le temps et de corriger les éventuelles erreurs.

Lorsqu'un modèle RBAC est utilisé et que les droits sont attribués à des groupes de comptes (représentant les rôles et profils), la revue doit commencer en vérifiant si les droits attribués à

chaque groupe correspondent au strict besoin opérationnel ; puis continuer en examinant l'association des comptes avec les groupes de comptes.

La revue de droits est faite de façon systématique, en prenant par exemple les besoins théoriques des utilisateurs et en les comparant à leurs droits d'accès effectifs sur les systèmes. Elle est également l'occasion de détecter des comptes qui doivent être désactivés (section 5.1.3), en comparant notamment avec les listes d'employés et de prestataires.

La revue de droits peut faire intervenir les responsables hiérarchiques. Ces derniers sont les plus à même de juger de l'appartenance d'un utilisateur ou d'un processus automatique à un groupe particulier, ou des droits associés à ce groupe.

Lorsque la solution de gestion de droits est complexe (annuaire d'entreprise comme Active Directory, progiciel de gestion intégré [29]), certains privilèges donnent le droit d'en attribuer d'autres, ou de contrôler certaines ressources permettant d'en acquérir d'autres. Dans ce cas, une analyse des chemins de contrôle et des chemins d'élévation de privilèges est recommandée, en recourant si nécessaire à des outils spécialisés.

29. Ou *entreprise resource planning (ERP)* en anglais.

6
Maintien en conditions de sécurité (règle 16)

Ce chapitre détaille les recommandations relatives à la section 3 du chapitre II de l'*arrêté du 14 septembre 2018*. Il couvre la règle relative aux procédures de ***maintien en conditions de sécurité*** (***MCS***, règle 16).

Maintien en conditions de sécurité (MCS)

Ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de sécurité d'un SI tout au long de son cycle de vie.

Objectif

Maintenir le SIE en conditions de sécurité dans le temps, en raccourcissant le délai entre la publication d'une vulnérabilité et l'adoption par l'opérateur de mesures techniques ou organisationnelles pour la contrer.

6.1 Procédure de maintien en conditions de sécurité

Des vulnérabilités sont susceptibles d'être révélées tout au long du cycle de vie d'un système. Les vulnérabilités non corrigées sont autant de points d'entrée potentiels pour permettre à un attaquant de compromettre un SI. L'exploitation des vulnérabilités peut même être rendue systématique et automatique, comme évoqué dans l'exemple d'attaque suivant.

Scénario d'attaque

Un attaquant utilise un outil d'inventaire réseau pour détecter quel système d'exploitation est utilisé sur un serveur, quels services y sont installés et les versions de ces services.
Ensuite, il recherche les vulnérabilités connues pour chaque version du service concerné et s'il existe un code malveillant développé pour exploiter cette vulnérabilité.
La recherche et le déploiement d'un code d'exploitation sont facilités par des outils tels que `Metasploit`.
À l'aide du code malveillant, il obtient un accès au serveur.

Il est donc nécessaire d'organiser le maintien en conditions de sécurité du SIE en accord avec la politique de sécurité des systèmes d'information de l'opérateur.

R58

⚖ Documenter une politique de MCS

L'opérateur doit élaborer et tenir à jour une politique de maintien en conditions de sécurité des ressources matérielles et logicielles de ses SIE, conformément à sa PSSI. Cette politique doit définir les procédures de veille de sécurité, de vérification des mises à jour et d'analyse de leurs impacts, les délais d'application des mises à jour et la gestion des exceptions.

La procédure de MCS doit décliner les besoins de sécurité exprimés dans la PSSI. Par exemple, si la PSSI décrit un système ou un type de technologie comme étant sensible, l'opérateur doit appliquer les délais adéquats de prise en compte des vulnérabilités signalées.

L'opérateur doit s'assurer que chaque SIE est couvert par une procédure de MCS dûment documentée. Il peut le faire sous la forme d'une procédure globale, applicable à tous les SIE ou à tous ses SI, ou sous la forme de plusieurs procédures distinctes si les conditions de mise en œuvre sont différentes selon les SIE.

Les procédures doivent être tenues à jour. Au minimum, elles doivent être mises à jour dès que la PSSI, l'analyse de risque ou l'architecture logicielle ou matérielle du SIE évoluent. Il est recommandé de définir une périodicité pour la revue des procédures.

Une fois l'inventaire des ressources logicielles et matérielles constitué (règle 6 relative à la cartographie), l'opérateur doit s'organiser pour être informé continuellement de nouvelles vulnérabilités affectant ces ressources et d'éventuels correctifs associés. Pour cela, l'opérateur doit mettre en place une veille de sécurité.

R59

⚖ Mettre en place une veille de sécurité

L'opérateur doit se tenir informé des vulnérabilités et des mesures correctrices de sécurité susceptibles de concerner les ressources matérielles et logicielles de ses SIE. Pour cela, il doit utiliser des sources de confiance, notamment les fournisseurs ou les fabricants des ressources concernées ou les centres de prévention et d'alerte en matière de sécurité numérique tels que le CERT-FR [30].

Le CERT-FR est donné en tant que référence publique, mais les opérateurs peuvent recourir aux services d'un autre centre de prévention et d'alerter ou effectuer leur propre veille, à condition de s'assurer de la couverture de l'ensemble des éléments de leurs SIE.

6.2 Application des mises à jour de sécurité

Une fois la procédure de MCS définie, il convient de la mettre en œuvre en appliquant les mises à jour. Ne sont traitées dans le cadre de ce guide que les éléments ayant un impact sur le niveau de sécurité du SIE, appelés *mises à jour de sécurité*, ce qui comprend les correctifs de sécurité et les mises à jour apportant une fonction de sécurité.

30. CERT-FR, centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, au sein de l'ANSSI. Site Web : https://www.cert.ssi.gouv.fr.

Pour l'application des mises à jour ne répondant pas à un besoin de sécurité (maintien en condition opérationnelle), le délai d'application peut changer et être plus long.

Exemple

Par exemple, la procédure de MCS du SIE prévoit l'application des correctifs de sécurité critiques sous 5 jours, celle des autres correctifs de sécurité sous 30 jours, et celle des mises à jour fonctionnelles une fois par an seulement.

6.2.1 Téléchargement de mises à jour fiables

Une fois informé d'une vulnérabilité et de la mise à disposition d'une mise à jour de sécurité, l'opérateur doit trouver une source fiable pour télécharger ce correctif. L'objectif est de s'assurer de l'intégrité et de l'authenticité de la mise à jour qui est appliquée au SIE.

R60

Obtenir des mises à jour de sécurité officielles

Il est fortement recommandé que l'opérateur s'assure de l'origine et de l'intégrité de toute nouvelle version ou mise à jour de sécurité avant son installation.
Si la mise jour de sécurité est signée, il est fortement recommandé que l'opérateur vérifie la signature.

L'échec du contrôle d'intégrité implique que la mise à jour a été modifiée. Elle peut donc être malveillante ou non fonctionnelle, et ne doit pas être appliquée.

6.2.2 Application des mises à jour

Une fois la mise à jour de sécurité téléchargée, il est fortement recommandé que l'opérateur en analyse l'impact des points de vue technique et opérationnel, avant de l'installer sur le SIE. Il peut le faire à l'aide d'une plate-forme de test représentative de l'environnement de production.

Enfin, l'opérateur doit planifier l'application de la mise à jour de sécurité dès qu'il en a connaissance. Le délai d'application n'est pas forcément générique et peut prendre de multiples valeurs en fonction du type de correctif à appliquer, de la criticité de la vulnérabilité, de la nature du SIE, de la criticité du SIE, de son niveau d'exposition, etc. ; la procédure de MCS doit fixer un délai maximum associé à chaque cas.

R61

Appliquer les mises à jour de sécurité

Une fois informé de la disponibilité d'une mise à jour, l'opérateur doit en planifier l'installation, en accord avec les délais fixés par la procédure de MCS du SIE.
Préalablement à l'installation, l'opérateur doit analyser l'impact de la mise à jour et prévoir les exceptions. Il est recommandé que l'opérateur définisse une procédure de retour à la version précédente en cas de problème lors de l'installation.

6.2.3 Gestion des systèmes obsolètes

Le corollaire de la recommandation de maintenir à jour un SIE est que ce dernier doit utiliser des versions pour lesquelles des mises à jour sont disponibles, c'est-à-dire des versions supportées.

R62

⚖ Utiliser des logiciels et des matériels supportés

Toutes les ressources matérielles et logicielles du SIE doivent être dans des versions supportées par leurs fournisseurs ou leurs fabricants.
Il est recommandé que l'opérateur mette en œuvre une gestion du cycle de vie de ces ressources pour en prévenir l'obsolescence.

Attention

Lors de la création du SIE et tout au long de son évolution, l'opérateur doit opter pour des versions de composants logiciels ou matériels qui seront supportées sur une période de temps couvrant celle probable de leur utilisation dans le SIE.

Dans certains cas, une difficulté technique ou organisationnelle peut retarder ou empêcher la mise à jour d'un SIE. Par exemple :

- sur un système isolé, il n'existe pas de connexion permettant le téléchargement des mises à jour. Les mises à jour de sécurité sont donc téléchargées à l'extérieur du SIE, puis intégrées dans le SIE suivant un processus manuel qui peut prendre plus de temps ;
- certains systèmes industriels doivent être arrêtés afin d'effectuer les mises à jour. Dans ce cas, on peut attendre la fenêtre de maintenance suivante ;
- si la nouvelle version d'un logiciel est incompatible avec le reste de l'infrastructure ou qu'elle demande un changement d'architecture, alors la mise à jour peut être retardée le temps de trouver une solution globale.

Dans un tel cas, l'opérateur doit donc mettre en place des mesures techniques ou organisationnelles prévues par la procédure de MCS pour réduire les risques liés à une version obsolète, et empêcher un attaquant de pouvoir exploiter une vulnérabilité dont il a connaissance. Ces mesures peuvent renforcer les mesures déjà exigées par la réglementation, comme le cloisonnement et le filtrage, en isolant le SIE utilisant des versions obsolètes.

R62 -

⚖ Pallier l'utilisation de versions obsolètes de logiciels et de matériels

Lorsque des raisons techniques ou organisationnelles retardent ou empêchent la mise à jour d'un SIE, l'opérateur doit mettre en place des mesures techniques ou organisationnelles prévues par la procédure de MCS pour réduire les risques liés à une version obsolète.
L'opérateur doit décrire les raisons, les mesures et leurs justifications dans le dossier d'homologation du SIE.
En particulier, il est recommandé de renforcer le cloisonnement et le filtrage entre le SIE et les autres SI, et au sein du SIE, en allant si possible jusqu'à l'***isolation*** des composants obsolètes.

Annexe A
Correspondance des règles NIS et LPM

Domaine NIS	Règles NIS	Correspondance dans la LPM
GOUVERNANCE	**Règle 1.** Analyse de risque	**Règle 2.** Homologation de sécurité, qui précise que l'analyse de risque fait partie du dossier d'homologation
	Règle 2. Politique de sécurité	**Règle 1.** Politique de sécurité des systèmes d'information
	Règle 3. Homologation de sécurité	**Règle 2.** Homologation de sécurité
	Règle 4. Indicateurs	**Règle 20.** Indicateurs
	Règle 5. Audits de la sécurité	**Règle 2.** Homologation de sécurité, qui précise que l'audit fait partie de la démarche d'homologation
	Règle 6. Cartographie	**Règle 3.** Cartographie
PROTECTION	**Règle 7.** Configuration	**Règle 19.** Installation de services et d'équipements
	Règle 8. Cloisonnement	**Règle 16.** Cloisonnement
	Règle 9. Accès distant	**Règle 18.** Accès à distance
	Règle 10. Filtrage	**Règle 17.** Filtrage
	Règle 11. Comptes d'administration	**Règle 14.** Comptes d'administration
	Règle 12. Systèmes d'information d'administration	**Règle 15.** Systèmes d'information d'administration
	Règle 13. Identification	**Règle 11.** Identification
	Règle 14. Authentification	**Règle 12.** Authentification
	Règle 15. Droits d'accès	**Règle 13.** Droits d'accès
	Règle 16. Procédure de maintien en conditions de sécurité	**Règle 4.** Maintien en conditions de sécurité
	Règle 17. Sécurité physique et environnementale	Sujet non abordé dans la LPM, les OIV ayant d'autres réglementations sur ce sujet
DÉFENSE	**Règle 18.** Détection	**Règle 7.** Détection
	Règle 19. Journalisation	**Règle 5.** Journalisation
	Règle 20. Corrélation et analyse de journaux	**Règle 6.** Corrélation et analyse de journaux
	Règle 21. Réponse aux incidents	**Règle 8.** Traitement des incidents de sécurité
	Règle 22. Traitement des alertes	**Règle 9.** Traitement des alertes
RÉSILIENCE	**Règle 23.** Gestion de crises	**Règle 10.** Gestion de crises

Annexe B
Glossaire

Accès à distance

Type d'accès dans lequel une ou plusieurs ressources non maîtrisées par l'opérateur sont utilisées à une quelconque étape de la connexion à un SI.

ACL

Access control list. En français : liste de contrôle d'accès.
Mécanisme de contrôle d'accès basé sur une liste de règles de ***filtrage***.
Par exemple, une ***ACL*** réseau filtre des flux réseau en se basant notamment sur des adresses IP.

Actions d'administration

Ensemble des actions d'installation, de suppression, de modification ou de consultation d'un système ou d'un automate participant au SI et susceptibles de modifier le fonctionnement ou la sécurité de celui-ci. Les actions de maintenance et de supervision sont incluses dans les ***actions d'administration*** dès lors qu'elles nécessitent des accès du même niveau de privilège que les ***actions d'administration***.

Administrateurs

Les ***administrateurs*** sont des utilisateurs du SI qui y effectuent des ***actions d'administration***.
Il est parfois pertinent de distinguer l'administration *technique* de l'administration *métier*. Cette dernière correspond à la gestion fine des droits au sein d'une application métier particulière.

Authentification

Processus ayant pour but de vérifier l'identité dont se réclame un utilisateur, un processus, une entité ou une machine. S'authentifier consiste à apporter la preuve de cette identité au moyen d'un ou plusieurs ***facteurs d'authentification***. L'authentification est donc précédée d'une ***identification***.

Authentification à double facteur

Authentification mettant en œuvre plusieurs types de ***facteurs d'authentification***, idéalement indépendants l'un de l'autre et de types différents. Un tel processus est plus difficile à contrefaire qu'une ***authentification*** basée sur un seul ***facteur d'authentification***, l'attaquant devant compromettre plusieurs secrets au lieu d'un seul. À aucun moment l'ensemble des facteurs requis ou leurs dérivés ne sont présents ou accessibles à un même système de traitement.
Exemple : carte à puce contenant un certificat et le mot de passe associé.

Bac à sable

Espace technique dédié complètement isolé du reste du SI et utilisé pour exécuter ou tester des actions potentiellement dangereuses afin qu'elles n'aient pas d'impact sur les autres SI.

Bad USB	En français : USB malveillant. Attaque dans laquelle l'attaquant connecte un matériel USB malveillant dont le micro-code a été modifié dans le but de tromper l'utilisateur sur la nature même du matériel. Ce support se fait généralement passer pour un périphérique USB classique, afin de contourner les éventuelles restrictions fixées sur la machine attaquée, puis tente de passer des commandes, de copier des fichiers, d'écouter le réseau, etc.
Besoin de fonctionnement (principe du ...)	Principe selon lequel chaque élément d'un SI ne peut accéder qu'aux autres éléments que s'il en a la nécessité impérieuse, dans le cadre d'une fonction déterminée, pour la bonne exécution d'une mission précise. Il peut s'agir d'un besoin métier ou purement technique.
Bring your own device	En français : apportez votre équipement personnel de communication (AVEC selon le Journal officiel du 24 mars 2013). Se dit de l'utilisation, dans un cadre professionnel, d'un matériel personnel tel qu'un téléphone multifonction ou un ordinateur.
BYOD	Voir ***bring your own device***.
Cloisonnement	Fonction de sécurité assurant une séparation entre les éléments d'un SI sans impact sur le service rendu. Elle se met en œuvre techniquement par une ***segmentation*** du système en ***sous-systèmes***. Cette démarche restreint chaque partie du SI aux actions dont elle a besoin.
Cloisonnement par le chiffre	Solution dans laquelle la fonction de ***cloisonnement*** est assurée par l'utilisation d'un mécanisme de chiffrement sur au moins un ensemble de données à cloisonner. Exemple : voir section 3.2.2.2.
Compte d'administration	Compte disposant de privilèges nécessaires aux ***actions d'administration*** et associé à un ***administrateur***.
Compte individuel	Compte correspondant à une seule personne physique, ou un seul processus automatique, identifiable par son nom ou un identifiant unique.
Compte partagé	Compte commun à plusieurs personnes ou plusieurs processus automatiques. Il ne permet pas d'associer de façon unique un compte et la personne ou le processus automatique qui l'utilise et donc d'assurer l'***imputabilité*** des actions.
Compte privilégié	Compte dont les ***droits d'accès*** permettent des actions qui ne sont pas autorisées à la majorité des utilisateurs de l'application ou du SI. C'est par exemple le cas d'un compte d'administrateur technique. Cela peut être aussi le cas d'un compte d'administrateur métier qui permet de définir les droits des autres utilisateurs dans une application.

Compte technique

Compte rattaché à un processus automatique (un programme, une application, un service, un script, etc.) et non une personne physique. Il s'agit d'un ***compte individuel*** ou d'un ***compte partagé***.

Confiance (de...)

Produits ou prestataires qui sont conformes à un référentiel ou à une cible de sécurité sur le périmètre qui a été évalué.

Confidentialité

Caractère réservé d'une information ou d'un traitement dont l'accès est limité aux seules personnes admises à la (le) connaître pour les besoins du service, ou aux entités ou processus autorisés.

Déplacement latéral

Action d'un attaquant qui a compromis une machine et qui teste ensuite l'ensemble des machines accessibles dans l'objectif de s'y propager.

Disponibilité

Propriété d'une information ou d'un traitement d'être utilisable à la demande par une personne ou par un système.

Environnement de travail

Ensemble de ressources logicielles regroupant les systèmes d'exploitation et les outils applicatifs mis à la disposition d'un utilisateur.
L'environnement de travail peut être sur un poste de travail physique, virtualisé (localement ou à distance), et peut inclure des éléments applicatifs présents sur des serveurs (consoles, rebonds, etc.).

Facteur d'authentification

Élément technique permettant de réaliser une ***authentification***, parmi :

- *Ce que l'utilisateur connaît* : l'élément secret est alors un mot de passe, un code PIN, etc. ;
- *Ce que l'utilisateur possède* : l'élément secret est alors un élément cryptographique protégé dans un support physique comme une carte à puce, une clé USB, etc. ;
- *Ce que l'utilisateur est* : l'élément secret est alors la modélisation mathématique de caractéristiques individuelles de l'utilisateur, notamment biométriques (structure de l'iris, empreinte digitale ou palmaire, etc.).
- Parfois, on ajoute « *ce que l'utilisateur sait faire* » (vitesse de frappe au clavier, façon de tracer une signature manuscrite, etc.).

Filtrage

Démarche visant à autoriser ou interdire des actions en fonction de règles préétablies ou construites automatiquement.

Force brute

Attaque dans laquelle un attaquant va tester successivement toutes les possibilités jusqu'à trouver celle permettant de déverrouiller le secret recherché.
L'attaque la plus fréquente prend pour cible les mots de passe.

Fournisseur de service numérique (FSN)

Personne morale qui fournit tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. Selon l'article 10 de la loi n°2018-133 du 26 février 2018 [3], trois types de services numériques sont concernés par le cadre réglementaire :

a) « Place de marché en ligne, à savoir un service numérique qui permet à des consommateurs ou à des professionnels [...] de conclure des contrats de vente ou de service en ligne avec des professionnels soit sur le site Web de la place de marché en ligne, soit sur le site Web d'un professionnel qui utilise les services informatiques fournis par la place de marché en ligne ;

b) Moteur de recherche en ligne, à savoir un service numérique qui permet aux utilisateurs d'effectuer des recherches sur [des sites Internet] sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé ;

c) Service d'informatique en nuage, à savoir un service numérique qui permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées. »

Identifiant

Élément par lequel une personne ou un processus automatique indique de façon explicite quelle identité lui est associée sur le SI.

Identification

Action d'un utilisateur ou d'un processus automatique consistant à communiquer une identité préalablement enregistrée.

Imputabilité

Capacité d'attribuer une action de façon certaine à un utilisateur ou à un processus automatique.

Intégrité

Propriété assurant qu'une information ou un traitement n'a pas été modifié ou détruit de façon non autorisée.

IPsec

Internet protocol security. En français : sécurité du protocole IP.
Cadre de standards permettant de sécuriser des communications IP. Par extension, cela désigne aussi un type de tunnel ***VPN*** chiffré et authentifié.

Isolation

Fait, pour un SI, de fonctionner en complète autarcie : pour remplir ses objectifs fonctionnels, le système se suffit à lui-même et n'entretient pas d'échanges avec d'autres systèmes. Il n'existe aucun lien permanent entre un SI isolé et d'autres SI.

Liste d'autorisation

Mécanisme de ***filtrage*** décrivant la liste des éléments autorisés et interdisant tous les autres.

Liste d'interdiction

Mécanisme de ***filtrage*** décrivant la liste des éléments interdits et autorisant tous les autres.

Maintien en conditions de sécurité

Ensemble des mesures organisationnelles et techniques concourant à maintenir le niveau de sécurité d'un SI tout au long de son cycle de vie.

Maîtrisé

Élément sous la responsabilité directe de l'opérateur.
Voir ***poste maîtrisé***, ***réseau maîtrisé***, ***SI maîtrisé*** et ***site maîtrisé***.

MCS

Voir ***maintien en conditions de sécurité***.

Moindre privilège (principe du ...)

Principe qui énonce qu'une activité ne doit bénéficier que des autorisations strictement nécessaires à l'exécution des actions dont l'utilité est avérée.

NIS **(directive)**

Network and Information system Security. En français : sécurité des réseaux et systèmes d'information (SRI). La directive ***NIS*** poursuit un objectif majeur : assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Elle a été adoptée par les institutions européennes le 6 juillet 2016.

Nomadisme (numérique)

Toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité.

Opérateurs d'importance vitale (OIV)

Selon le code de la Défense, art. L-1332-1, « opérateurs publics ou privés exploitant des établissements ou utilisant des installations et ouvrages, dont l'indisponibilité risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la nation ». Les OIV sont désignés par les ministères ou les préfets de département.

Opérateurs de services essentiels (OSE)

Selon l'article 5 de la loi n°2018-133 du 26 février 2018 [3], « opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services ». Les OSE sont désignés par le Premier ministre.

OSE

Voir ***opérateurs de services essentiels***.

Poste d'administration

Terminal matériel, fixe ou portable, utilisé par les ***administrateurs*** pour les ***actions d'administration***.

Poste maîtrisé

Poste de travail fourni, configuré et maintenu par l'opérateur. D'une part, il ne peut s'agir d'un équipement personnel (voir ***BYOD***) et d'autre part, l'utilisateur ne peut être ***administrateur*** du poste, le niveau de sécurité pouvant alors être directement modifié par l'utilisateur.

Proxy

En français : serveur mandataire.
Serveur installé en coupure d'un flux sortant du SI pour isoler la prise en charge d'un requête du reste du SI. Un ***reverse proxy*** a la même action sur les flux entrants.
Ce serveur ***proxy*** permet d'apporter plusieurs mesures de sécurité :

- il ne présente qu'une seule machine à l'extérieur pour tous les flux sortants et masque donc l'architecture interne ;
- il ne ré-émet que les requêtes autorisées ;
- il peut modifier une requête reçue de sorte que la requête ré-émise soit nettoyée de certains codes malveillants liés à la pile protocolaire ;
- etc.

PSSI

Politique de sécurité des systèmes d'information.

***RBAC* (méthodologie ou modèle...)**

Role-based access control. En français : contrôle d'accès basé sur des rôles.
Approche de gestion des accès basée sur le regroupement des ***droits d'accès*** en rôles et profils dans le but d'attribuer systématiquement le même ensemble de ***droits d'accès*** aux utilisateurs ayant les mêmes besoins.

Réseau et système d'information

Selon l'article 1 de la loi n°2018-133 du 26 février 2018 [3] :

1° tout réseau de communications électroniques tel que défini au 2° de l'article L. 32 du code des postes et des communications électroniques ;

2° tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques ;

3° les données numériques stockées, traitées, récupérées ou transmises par les éléments mentionnés aux 1° et 2° du présent article en vue de leur fonctionnement, utilisation, protection et maintenance.

Réseau maîtrisé

Réseau possédé et opéré complètement par l'opérateur.
Voir à l'inverse ***réseau tiers***.

Réseau privé virtuel

Mécanisme de réseau dans lequel un protocole d'encapsulation crée deux réseaux logiques distincts bien qu'ils partagent les mêmes supports physiques.
L'ANSSI recommande d'utiliser des réseaux privés virtuels chiffrés et authentifiés, comme ***IPsec***. Les fonctions de chiffrement et d'authentification ne sont pas en effet présentes par défaut sur tous ces réseaux. Les VRF, par exemple, sont des VPN réseau qui ne sont ni chiffrés ni authentifiés.

Réseau tiers

Réseau qui n'est pas ***maîtrisé*** par l'opérateur.
Des exemples de ***réseau tiers*** sont Internet, un réseau d'un opérateur de télécommunications ou un réseau non maîtrisé d'une entreprise tierce.
Cependant, un réseau non maîtrisé peut être considéré comme n'étant pas un ***réseau tiers***, si les deux conditions suivantes sont strictement respectées :

- il s'agit d'une liaison entre deux ***sites maîtrisés*** de l'opérateur ;
- des moyens contrôlés par l'opérateur sont mis en œuvre pour encapsuler tous les flux directs ou indirects à destination du SIE, dans un ***VPN*** de type ***IPsec*** configuré suivant les recommandations de l'ANSSI et sans possibilité technique de contournement.

Reverse proxy

En français : serveur mandataire inverse.
Voir ***proxy***.

Sas (d'import de données)

Dispositif connecté au réseau opérationnel dont l'objectif est de garantir l'innocuité du média amovible et des données transférées à destination de ce réseau.

Sécurité des réseaux et systèmes d'information

Selon l'article 1 de la loi n°2018-133 du 26 février 2018 [3], « la sécurité des réseaux et systèmes d'information consiste en leur capacité de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles. »

Segmentation

Subdivision d'un SI en différents éléments, parfois appelés ***sous-systèmes***. Pour le réseau, cela peut correspondre à la création de sous-réseaux IP, de ***VLAN*** ou de ***VPN***. En cas de segmentation physique, lorsque qu'aucun élément physique n'est commun à plusieurs ***sous-systèmes***, on peut parler de cloisonnement physique.

Sensibilité

Caractère de ce qui a un besoin de sécurité spécifique. Un niveau de ***sensibilité*** d'un SI supérieur à celui des autres SI de l'opérateur nécessite des mesures de sécurité supplémentaires.
Le niveau de ***sensibilité*** d'un SI est fonction :

- d'une réglementation spécifique ;
- d'une criticité métier ;
- de besoins en ***disponibilité***, ***intégrité***, ***confidentialité*** et ***traçabilité***.

Service numérique

Selon l'article 10 de la loi n°2018-133 du 26 février 2018 [3], « tout service fourni normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services. »

SI administré	Ensemble des éléments du SI que l'***administrateur*** doit administrer. Il peut s'agir de postes de travail, de serveurs, d'hyperviseurs, d'équipements réseau, d'équipements de stockage, etc.
SI d'administration	SI utilisé pour administrer des ressources qui sont présentes dans un autre SI, dit ***SI administré*** et distinct du ***SI d'administration***.
SI maîtrisé	SI dont les éléments constitutifs sont connus, configurés et maintenus par l'opérateur ou par un de ses prestataires, et permettent de garantir le niveau de sécurité du SI.
SIE	Système d'information essentiel.
Site maîtrisé	Site sous la responsabilité de l'opérateur et localisé dans une enceinte physiquement protégée.
Sous-système (d'un SI)	Un ou plusieurs éléments d'un SI qui répondent à un même besoin fonctionnel, aux mêmes critères de sécurité (même niveau de sécurité des données et des traitements, ***disponibilité***, ***intégrité***, ***confidentialité***) et qui présentent le même niveau d'exposition (accessible à des utilisateurs, système isolé, etc.). Ces éléments homogènes sont administrés par des ***administrateurs*** de même niveau de confiance.
Statification	Mécanisme visant à rendre inoffensif un fichier contenant du texte, donc potentiellement du code interprétable ou exécutable, en le convertissant dans un autre format, en général une image.
Station blanche	Dispositif isolé d'un SI opérationnel dont l'objectif est de garantir l'innocuité du média amovible et des données transférées à destination du SI opérationnel.
Surface d'attaque	L'ensemble des éléments techniques du SI qui pourraient être utilisés pour réaliser une attaque. Une ***surface d'attaque*** est d'autant plus large que le nombre d'éléments est grand ou que ces derniers présentent de vulnérabilités exploitables par un attaquant.
Télétravail	Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication (article L. 1222-9 du code du travail). Le télétravail est une forme de ***nomadisme numérique***.
TLS	*Transport layer security*. En français : sécurité de la couche de transport. Protocole de sécurisation des échanges, évolution du protocole SSL.
Traçabilité	Caractère d'un SI dont il est possible de retrouver l'historique de fonctionnement.

USB killer

En français : tueur d'USB.
Attaque dans laquelle l'attaquant utilise un support malveillant pour envoyer une décharge électrique sur un port USB, rendant indisponible ce port, voire l'ensemble de la carte-mère.

VLAN

Virtual local area network. En français : réseau local virtuel.

VPN

Virtual private network. En français : ***réseau privé virtuel***.

Vulnérabilité

Faute, par malveillance ou maladresse, dans les spécifications, la conception, la réalisation, l'installation ou la configuration d'un système, ou dans la façon de l'utiliser. Une ***vulnérabilité*** peut être utilisée par un code d'exploitation et conduire à une intrusion dans le système.

Annexe C
Mise en œuvre technique du cloisonnement

Suivant le type d'élément technique à cloisonner (système, réseau, stockage), les recommandations R11, R11- et R11-- peuvent être mises en œuvre de différentes façons.

C.1 Cloisonnement dans le domaine des systèmes

Cette section s'intéresse aux éléments de SI installés sur une machine physique : systèmes d'exploitation, logiciels d'infrastructure, applications, etc.

C.1.1 Cloisonnement physique

Dans le cas d'un cloisonnement physique, on suppose que la machine physique n'est utilisée que pour une fonction. Sa compromission ne touche donc que cette seule fonction. Tout autre système ou toute autre application est hébergée sur une machine physique différente.

Exemple

Un SIE contient deux serveurs Web, l'un accessible depuis le réseau public et l'autre accessible uniquement depuis un réseau local. Leur différence d'exposition conduit à les cloisonner en deux sous-systèmes.
Il est recommandé de les installer sur deux machines physiques différentes. Ainsi, la compromission d'une des machines ne peut s'étendre à l'autre que si elles sont toutes deux connectées au même réseau, d'où l'importance du cloisonnement réseau (section C.2) et du filtrage réseau (section 3.4).

C.1.2 Cloisonnement logique par le chiffre

Dans le cas d'un cloisonnement logique par le chiffre, plusieurs éléments sont mutualisés sur la même machine physique et un outil de chiffrement assure que la compromission d'un élément ne compromet pas la confidentialité et l'intégrité des données des autres.

Attention

Les exemples de cloisonnement par le chiffre au niveau système sont très rares.

En effet, dès que l'information est accessible en clair sur un système par un processus qui y a légitimement accès, alors le cloisonnement ne repose plus sur le chiffre mais

sur des mécanismes logiques de contrôle d'accès à la mémoire. Ce cas se rencontre fréquemment : chiffrement d'un disque (le disque est déchiffré lorsqu'il est monté au niveau du système d'exploitation), chiffrement d'une machine virtuelle sur le stockage (la machine virtuelle est déchiffrée avant d'être exécutée).

Certaines implémentations déplacent la gestion du chiffrement jusqu'au niveau du processeur (ex. : la technologie SEV d'AMD, qui n'a pas été évaluée par l'ANSSI), mais restent finalement dépendantes d'une intégration correcte avec l'hyperviseur qui les pilotent - et donc d'un cloisonnement logique simple.

Un des rares exemples pertinents est celui du chiffrement homomorphe des données [31]. Dans ce cas, les données sont chiffrées sur un premier serveur, puis manipulées sur un second serveur par un processus qui effectue des calculs sur ces données, sans les déchiffrer et donc sans les exposer aux autres processus partageant ce serveur.

C.1.3 Cloisonnement logique simple

Si l'opérateur décide de mettre en oeuvre un cloisonnement logique simple, il doit déterminer quelles ressources il souhaite mutualiser sur une machine physique et quels mécanismes logiques assurent la fonction de cloisonnement.

Exemple

Quelques exemples de mécanismes logiques permettant de cloisonner des applications partageant une même machine physique :

- avoir plusieurs machines virtuelles, chacune hébergeant un système d'exploitation et une application, exécutées par un hyperviseur ;
- avoir, au sein d'un même système d'exploitation, plusieurs espaces d'exécution (comme des conteneurs) dédiés chacun à une application ;
- avoir des services différents, exécutés par des comptes distincts, au sein d'un même système d'exploitation.

Dans ce cas, la machine physique et certaines couches logicielles (hyperviseur, OS, etc.) sont mutualisées entre plusieurs fonctions et la compromission de l'une de ces fonctions augmente les possibilités d'attaque des autres fonctions. Ce type de cloisonnement n'est pas recommandé pour des fonctions de niveaux de sensibilité ou d'exposition homogènes.

Information

Il existe des hyperviseurs ayant obtenu une certification de sécurité, comme le système PR/SM d'IBM certifié par l'office fédéral de la sécurité des technologies de l'information allemand (BSI).

31. Voir par exemple : https://fr.wikipedia.org/wiki/Chiffrement_homomorphe.

C.1.4 Complémentarité des types de cloisonnement système

L'exemple suivant montre l'emploi de plusieurs types de cloisonnement système, dans une démarche de défense en profondeur.

Exemple

Il est possible d'envisager un SIE minimal exécuté sur une seule et unique machine physique, ce qui permet d'avoir un cloisonnement physique entre le SIE et les autres SI.
Sur cette machine physique, il est ensuite possible d'installer un hyperviseur qui héberge plusieurs machines virtuelles, une par sous-système du SIE. Chaque machine virtuelle est donc cloisonnée logiquement des autres.
Enfin, dans chaque machine virtuelle, il est possible d'utiliser des serveurs applicatifs différents pour cloisonner entre elles des applications qui ont le même niveau de sensibilité mais qui sont ouvertes par exemple à des utilisateurs différents.

Pour plus de détails, le lecteur peut se reporter au *recommandations pour la mise en place de cloisonnement système* [39] de l'ANSSI.

C.2 Cloisonnement dans le domaine des réseaux

C.2.1 Cloisonnement physique

Pour un réseau, le cloisonnement physique est mis en œuvre en dédiant du matériel (câblage, équipements actifs comme les commutateurs et les pare-feux) à chaque sous-système à cloisonner. Cette solution est la plus sécurisée.

Le cloisonnement physique des réseaux peut s'accompagner :

- soit de l'absence totale d'interconnexion du SIE avec d'autres SI. On parle alors d'un SIE isolé. L'expression anglaise *air gap* désigne également cette architecture ;
- soit de l'existence d'interconnexions réalisées au moyen de diodes réseau permettant de garantir l'unidirectionnalité du flux d'information, du SIE vers les autres SI (pour une protection en intégrité et en disponibilité du SIE). Le niveau d'assurance de la fonction d'unidirectionnalité est dépendant de la technologie mise en oeuvre au sein de la diode réseau ; par exemple une diode optique apporte *a priori* un niveau d'assurance supérieur à une diode mettant en œuvre un contrôle des flux par circuit logique programmable (FPGA) ;
- soit finalement de la présence d'interconnexion avec un dispositif de filtrage tel qu'un pare-feu. Ce dernier cas relève alors d'un cloisonnement logique simple.

C.2.2 Cloisonnement logique par le chiffre

L'opérateur peut aussi utiliser le même réseau physique pour porter à la fois des flux de données d'un SIE et ceux d'autres SI. Dans ce cas, il possible de cloisonner ces flux en mettant en œuvre un cloisonnement logique par le chiffre.

Exemple

L'opérateur peut utiliser un même réseau physique pour transporter des tunnels ***VPN*** chiffrés et authentifiés pour des flux de sensibilités différentes, par exemple avec le protocole ***IPsec***.

Information

Dans le cas d'un tunnel ***IPsec***, l'opérateur peut obtenir une alternative acceptable à un cloisonnement physique en respectant strictement les *recommandations de sécurité relatives à IPsec* [24] de l'ANSSI.

Le chiffrement peut être appliqué depuis l'émetteur jusqu'au destinataire du flux, comme dans le cas d'un chiffrement applicatif type HTTPS. Le chiffrement peut aussi être appliqué uniquement sur une partie du trajet lorsque le flux traverse un réseau de moindre confiance, comme dans le cas d'un tunnel IPsec reliant deux réseaux à travers un réseau tiers. Les deux possibilités peuvent être combinées, réalisant du chiffrement multiple : par exemple, des commandes d'administration envoyées chiffrées par SSH transitant sur un réseau d'administration logique chiffré par IPsec.

C.2.3 Cloisonnement logique simple

Un cloisonnement logique d'un niveau de sécurité moindre peut être fait au niveau du réseau, sans chiffrement.

Exemple

L'opérateur peut définir des réseaux logiques sur un même réseau physique au moyen de VLAN ou de VRF [32].
Un cloisonnement par VLAN ou VRF n'est cependant pas recommandé comme unique moyen de cloisonnement, puisque le cloisonnement repose alors sur la bonne configuration et la robustesse de l'ensemble des équipements traversés.

Information

Au sujet des bonnes pratiques de configuration des VLAN, le lecteur peut consulter les *recommandations pour la sécurisation d'un commutateur de desserte* [10] de l'ANSSI.
Le lecteur intéressé par un exemple d'application des principes du cloisonnement réseau peut consulter le chapitre 2.4, « Architecture détaillée », du guide *recommandations relatives à l'interconnexion d'un système d'information à Internet - v2.0* [31] de l'ANSSI.
Enfin, il est rappelé que le cloisonnement logique du réseau doit s'accompagner de filtrage pour apporter un gain réel de sécurité.

32. *Virtual routing and forwarding* : technologie qui permet à plusieurs instances d'une table de routage de coexister dans le même routeur en même temps.

C.2.4 Complémentarité des types de cloisonnement réseau

Appliqués à un réseau mutualisé, le principe de défense en profondeur et l'efficacité économique peuvent amener à combiner le cloisonnement physique, le cloisonnement par le chiffre et le cloisonnement logique simple pour répondre à différentes contraintes et menaces.

Exemple

Dans un SIE, le réseau d'administration peut être physiquement distinct du réseau de production (cloisonnement physique). Au sein de ce réseau d'administration, plusieurs VLAN sont définis pour isoler des groupes de ressources administrées, et le mécanisme de PVLAN (*private VLAN*) est activé sur chaque VLAN pour empêcher le rebond entre les ressources administrées (cloisonnement logique simple). Enfin, l'administration des ressources se fait via des protocoles chiffrés (cloisonnement logique par le chiffre).

C.3 Cloisonnement dans le domaine du stockage

C.3.1 Cloisonnement physique

Un système de stockage peut être physiquement dédié à un serveur. C'est le cas pour des disques internes au serveur ou pour une baie à attachement direct (*direct-attached storage*).

Le système de stockage peut être aussi partagé entre plusieurs serveurs. Ce système de stockage peut être un équipement de type serveur de stockage en réseau (*network-attached storage* ou NAS) ou bien un système composé d'un réseau spécialisé (*storage area network* ou SAN).

Un système de stockage physique peut être commun à un ensemble de SI de même niveau de sensibilité : plusieurs SIE du même opérateur, ou plusieurs SI sensibles.

Attention

Il est aussi possible de dédier une partie seulement d'un système de stockage à un SI, comme un ensemble de disques dédié à un SIE dans une baie pourtant mutualisée.

Parce qu'il existe dans ce cas un composant mutualisé (ici, le contrôleur de la baie), l'efficacité du cloisonnement repose d'abord sur la robustesse du logiciel de ce composant. Il ne s'agit donc pas d'un cloisonnement physique, mais d'un cloisonnement logique simple, d'un niveau de confiance moindre.

C.3.2 Cloisonnement logique par le chiffre

Dans un cloisonnement logique par le chiffre, chaque sous-système dispose d'un espace logique chiffré au sein du système de stockage.

La recommandation R12 rappelle que le chiffrement doit être appliqué en amont du stockage, par les systèmes propriétaires des données, et non pas sur le système de stockage lui-même.

C.3.3 Cloisonnement logique simple

Pour un système de stockage, le cloisonnement logique simple consiste à contrôler l'accès à une ressource de stockage en fonction de critères logiques.

Exemple

- Le mécanisme de *zoning* permet de configurer quelles sont les ressources visibles ou accessibles aux hôtes dans un SAN. Il est mis en œuvre par les commutateurs du SAN.
- Le mécanisme de *LUN masking* permet de configurer quelles unités logiques (LUN) sont accessibles aux contrôleurs hôtes de bus (*host bus adapters* ou HBA). Il est mis en œuvre par les contrôleurs des baies de stockage.
- Le contrôle d'accès en lecture et en écriture aux partitions exposées par un NAS est lui aussi logique. Il s'appuie sur des éléments d'authentification présentés par les clients et est mis en œuvre par le serveur NAS.

C.3.4 Complémentarité des types de cloisonnement pour le stockage

Le principe de défense en profondeur et l'efficacité économique peuvent amener à combiner plusieurs types de cloisonnement sur un système de stockage partagé : cloisonnement physique, cloisonnement logique par le chiffre et cloisonnement logique simple. Cette combinaison répond à des menaces variées. Par exemple :

- S'il est parfois difficile de justifier économiquement de dédier un système de stockage à chacun des SIE, il peut être plus facile de déployer deux systèmes indépendants (SAN et baie) pour cloisonner physiquement d'un côté le stockage des SI sensibles de l'entité (dont les SIE) et de l'autre celui des SI moins sensibles.
- Au niveau de chaque système de stockage physique, un premier niveau de segmentation est apporté par du cloisonnement logique simple par *zoning* et *LUN masking*. Chaque hôte n'a en théorie accès qu'aux unités logiques dont il a besoin.
- Le chiffrement des données par les hôtes, en amont du système de stockage, complète le dispositif de protection en garantissant que les données en clair ne sont accessibles qu'à l'hôte qui les a chiffrées.
- Si le chiffrement par les hôtes n'est pas possible, le chiffrement des données par la baie avant écriture sur les disques permet de se prémunir contre une fuite de données en cas de vol ou de perte des médias de stockage.

Liste des recommandations

Bibliographie

[1] *Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*.
Directive (UE) 2016/1148, Union européenne, juillet 2016.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016L1148.

[2] *Règlement d'exécution (UE) 2018/151 de la Commission du 30 janvier 2018 portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en compte par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.*
Règlement d'exécution (UE) 2018/151, Union européenne, janvier 2018.
https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R0151.

[3] *Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*.
Loi n°2018-133, Légifrance, février 2018.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772.

[4] *Décret n°2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de services numériques*.
Décret n°2018-384, Légifrance, mai 2018.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036939971.

[5] *Arrêté du 13 juin 2018 fixant les modalités des déclarations prévues aux articles 8,11 et 20 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique*.
Arrêté du 13 juin 2018, Légifrance, juin 2018.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037102068.

[6] *Arrêté du 14 septembre 2018 fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique*.
Arrêté du 14 septembre 2018, Légifrance, septembre 2018.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037444012.

[7] *Loi n°2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale*.
Loi n°2013-1168 du 18 décembre 2013, Légifrance, décembre 2013.
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028338825.

[8] *Recommandations de sécurité relatives aux mots de passe*.
Note technique DAT-NT-001/ANSSI/SDE/NP v1.1, ANSSI, juin 2012.
https://www.ssi.gouv.fr/mots-de-passe.

[9] *Recommandations pour un usage sécurisé d'(Open)SSH*.
Note technique DAT-NT-007/ANSSI/SDE/NP v1.2, ANSSI, août 2015.
https://www.ssi.gouv.fr/nt-ssh.

[10] *Recommandations pour la sécurisation d'un commutateur de desserte*.
Note technique DAT-NT-025/ANSSI/SDE/NP v1.0, ANSSI, juin 2016.
https://www.ssi.gouv.fr/nt-commutateurs.

[11] *Recommandations de configuration d'un système GNU/Linux*.
Guide Version 1.2, ANSSI, février 2019.
https://www.ssi.gouv.fr/reco-securite-systeme-linux.

[12] *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*.
Guide Version 1.3, ANSSI, novembre 2017.
https://www.ssi.gouv.fr/guide-dns.

[13] *Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux*.
Guide Version 1.0, ANSSI, août 2018.
https://www.ssi.gouv.fr/guide-802-1X.

[14] *Maîtriser les risques de l'infogérance. Externalisation des systèmes d'information*.
Guide Version 1.0, ANSSI, décembre 2010.
https://www.ssi.gouv.fr/infogerance.

[15] *Passeport de conseils aux voyageurs*.
Guide Version 3.0, ANSSI, mai 2019.
https://www.ssi.gouv.fr/bonnes-pratiques-professionnels-en-deplacement.

[16] *Guide d'hygiène informatique : renforcer la sécurité de son système d'information en 42 mesures*.
Guide Version 2.0, ANSSI, septembre 2017.
https://www.ssi.gouv.fr/hygiene-informatique.

[17] *Guide pour l'élaboration d'une politique de sécurité des systèmes d'information*.
Guide Version 1.0, ANSSI, mars 2004.
https://www.ssi.gouv.fr/pssi.

[18] *Élaboration des tableaux de bord de la SSI*.
Guide Version 1.0, ANSSI, février 2004.
https://www.ssi.gouv.fr/tbssi.

[19] *Le guide des bonnes pratiques de configuration de BGP*.
Guide Version 1.0, ANSSI, septembre 2013.
https://www.ssi.gouv.fr/bonnes-pratiques-bgp.

[20] *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*.
Note technique DAT-NT-012/ANSSI/SDE/NP v1.0, ANSSI, décembre 2013.
https://www.ssi.gouv.fr/journalisation.

[21] *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-006/ANSSI/SDE/NP v1.0, ANSSI, mars 2013.
https://www.ssi.gouv.fr/politique-filtrage-parefeu.

[22] *La cybersécurité des systèmes industriels - Méthode de classification et mesures principales*.
Guide Version 1.0, ANSSI, janvier 2014.
https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels.

[23] *L'homologation de sécurité en neuf étapes simples*.
Guide Version 1.2, ANSSI, juin 2014.
https://www.ssi.gouv.fr/guide-homologation-securite.

[24] *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*.
Note technique DAT-NT-003/ANSSI/SDE/NP v1.1, ANSSI, août 2015.
https://www.ssi.gouv.fr/ipsec.

[25] *Recommandations et méthodologie pour le nettoyage d'une politique de filtrage réseau d'un pare-feu*.
Note technique DAT-NT-032/ANSSI/SDE/NP v1.0, ANSSI, août 2016.
https://www.ssi.gouv.fr/nettoyage-politique-fw.

[26] *Recommandations sur le nomadisme numérique*.
Guide ANSSI-PA-054 v1.0, ANSSI, octobre 2018.
https://ssi.gouv.fr/nomadisme-numerique.

[27] *Recommandations relatives à l'administration sécurisée des systèmes d'information*.
Guide Version 2.0, ANSSI, avril 2018.
https://www.ssi.gouv.fr/securisation-admin-si.

[28] *Recommandations de sécurité relatives à TLS*.
Guide Version 1.2, ANSSI, mars 2020.
https://www.ssi.gouv.fr/nt-tls.

[29] *Cartographie du système d'information*.
Guide Version 1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/administration/guide/cartographie-du-systeme-dinformation.

[30] *La méthode EBIOS Risk Manager - Le Guide*.
Guide Version 1.0, ANSSI, octobre 2018.
https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide.

[31] *Recommandations relatives à l'interconnexion d'un système d'information à Internet*.
Guide Version 3.0, ANSSI, juin 2020.
https://www.ssi.gouv.fr/passerelle-interconnexion.

[32] *Maîtrise du risque numérique - l'atout confiance*.
Guide Version 1.0, ANSSI, novembre 2019.
https://www.ssi.gouv.fr/administration/guide/maitrise-du-risque-numerique-latout-confiance.

[33] *Maîtriser la SSI pour les systèmes industriels*.
Guide Version 1.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/guide/la-cybersecurite-des-systemes-industriels.

[34] *Référentiel général de sécurité (RGS)*.
Référentiel Version 2.0, ANSSI, juin 2012.
https://www.ssi.gouv.fr/rgs.

[35] *Prestataires d'audit de la sécurité des systèmes d'information. Référentiel d'exigences*.
Référentiel Version 2.1, ANSSI, octobre 2015.
https://www.ssi.gouv.fr/referentiel-passi.

[36] *Prestataires de détection des incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf.

[37] *Prestataires de réponse aux incidents de sécurité. Référentiel d'exigences*.
Référentiel Version 2.0, ANSSI, août 2017.
https://www.ssi.gouv.fr/uploads/2014/12/pris_referentiel_v2.0.pdf.

[38] *Prestataires d'administration et de maintenance sécurisées. Référentiel d'exigences*.
Référentiel Version 0.9, ANSSI, octobre 2019.
https://www.ssi.gouv.fr/uploads/2019/10/anssi-pams-referentiel_exigences-v0.9.pdf.

[39] *Recommandations pour la mise en place de cloisonnement système*.
Guide Version 1.0, ANSSI, décembre 2017.
https://www.ssi.gouv.fr/guide-cloisonnement-systeme.

[40] *Licence ouverte / Open Licence v2.0*.
Page web, Mission Etalab, 2017.
https://www.etalab.gouv.fr/licence-ouverte-open-licence.

ANSSI-PA-085
Version 1.0 - 18/12/2020

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP
www.ssi.gouv.fr / conseil.technique@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
SGDSN