Architectures sécurisées

La collection de fiches « ReCyF en pratique » a pour objectif d'éclairer les principales mesures de gestion de risque issues du Référentiel Français de Cybersécurité (ReCyF). Ce référentiel a pour vocation de devenir le socle de la réglementation cyber française.

La collection de fiches « ReCyF en pratique » ne se substitue pas au référentiel. Les fiches ne sont pas prescriptives et ne visent pas l'exhaustivité. Sur la base des objectifs de sécurité fixés dans Référentiel Cyber France (ReCyF), ces fiches expliquent en pratique les effets recherchés, présentent des exemples concrets d'implémentation et proposent des références utiles pour aider les entités à mettre en œuvre ces objectifs et mesures de sécurité.

Elles s'adressent à un public technique chargé de la mise en œuvre de ces objectifs de sécurité au sein des entités concernées.

Cet ensemble de fiches est organisé en cinq rubriques: Défense, Protection, Gouvernance, Résilience et Obligations NIS 2, les quatre premières constituant les piliers essentiels des mesures de gestion des risques.

Rubrique Protection
Adoptez un ensemble de mesures essentielles pour éviter la compromission de vos SI.

INDICATION DE LECTURE

Pour distinguer les passages du texte destinés aux entités importantes (EI), de ceux destinés aux entités essentielles (EE), les marques suivantes ont été placées en marge du texte:

Ce texte (sans repère en marge) est à destination des EI et des EE

Ce texte (avec repère bleu en marge) est à destination des EE uniquement

Effets recherchés

L'architecture sécurisée d'un système d'information (SI) vise, en fonction des menaces identifiées, non seulement à prévenir les intrusions, mais aussi à les détecter, voire y remédier au cas où les protections mises en œuvre seraient défaillantes, compromises ou inefficaces face à un type d'attaque.

L'exposition désigne le niveau de visibilité et d'accessibilité d'un système ou d'un service face à des acteurs externes ou internes. La latéralisation est le fait, pour un attaquant, de se déplacer d'une zone ou d'un système compromis vers d'autres au sein du même système d'information. Le cloisonnement consiste alors à mettre en œuvre des mesures de sécurité entre différentes zones de sécurité constituant le SI et ainsi limiter leur exposition et la propagation d'un code malveillant ou la latéralisation d'un attaquant.

Le filtrage limite strictement les communications entre zones de sécurité aux seuls flux nécessaires et autorisés. Il facilite la détection des comportements anormaux, puisque toute communication inhabituelle devient plus visible dans un environnement où les flux autorisés sont explicitement définis.

Enfin, la sécurité des accès distants vise à proposer des mesures adaptées pour des contextes d'usage croissants où la sécurité physique des utilisateurs et de leurs équipements d'accès n'est pas garantie par défaut.

Combinés, le cloisonnement, le filtrage et la sécurité des accès distants réduisent la surface d'attaque du SI, évitent l'exposition inutile de ressources et garantissent que chaque utilisateur, application ou système n'accède qu'aux données nécessaires à sa mission.

Approche générale

CLOISONNEMENT

Mesures ReCyF	**Objectif de sécurité 7 :** Sécurisation de l'architecture des systèmes d'information ▸ Cloisonnement : 7.A.1-EI/EE, 7.A.2-EE, 7.A.3-EE, 7.A.4-EE, 7.A.5-EE, 7.A.6-EE, 7.A.7-EI/EE, 7.A.8-EE

Dans la vie courante, cloisonner signifie diviser un espace par des cloisons. Par exemple, on peut cloisonner un grand espace en plusieurs pièces plus petites.

Un cloisonnement minimal est de considérer que le SI doit être séparé de tout ce qui est extérieur au SI, comme Internet ou des SI d'autres entités (ex. : fournisseurs, partenaires). C'est l'équivalent d'avoir des murs pour délimiter l'intérieur d'une maison par rapport à l'extérieur. Les murs extérieurs, en général accompagnés d'une porte d'entrée principale, permettent de maîtriser qui rentre et qui sort de la maison. Ce cloisonnement minimal est appelé le **cloisonnement périmétrique.**

Une fois ce cloisonnement périmétrique mis en œuvre, il est souvent pertinent d'aller plus loin et de réfléchir si l'intérieur du SI peut être divisé, cloisonné. C'est l'équivalent d'avoir des cloisons à l'intérieur d'une maison pour en délimiter ses pièces. C'est le **cloisonnement interne.**

En informatique, cloisonner un SI signifie le diviser en plusieurs parties, appelées sous-systèmes ou zones de sécurité. Il se fait là aussi au niveau périmétrique et au niveau interne. Le moyen pour séparer les zones de sécurité, l'équivalent des cloisons, varie suivant le type de ressources. Les détails de ces modes de cloisonnement selon les types de ressources sont décrits ci-dessous.

Présentation des concepts

Cette section présente les concepts associés à la mise en œuvre du cloisonnement.

Comme introduit, le cloisonnement peut être périmétrique ou interne.

- Le **cloisonnement périmétrique** est autour du système d'information. Il délimite la frontière entre le SI de l'entité et les autres SI.

- Le **cloisonnement interne** est celui réalisé à l'intérieur du SI de l'entité. Ce cloisonnement délimite plusieurs sous-systèmes, ou zones de sécurité, au sein du SI.

Les sous-systèmes ou **zones de sécurité** sont les subdivisions internes au SI de l'entité. Une zone de sécurité (dénommée simplement « zone » ultérieurement) représente un ensemble d'environnements (systèmes, applications, traitements, etc.) évalués comme homogènes du point de vue de leur exposition, de leur sensibilité et de leur niveau de sécurité :

- L'exposition de la zone : par exemple, la zone est-elle exposée à Internet, ou uniquement accessible depuis d'autres zones internes du SI ?

- La sensibilité de la zone : y a-t-il des enjeux de sécurité faibles ou importants ? Par exemple, les données hébergées sont-elles réglementées ou stratégiques pour la survie de mon entité ?

- Le niveau de sécurité de la zone : la zone contient-elle des équipements vulnérables, obsolètes ou difficiles à sécuriser, ou bien des équipements modernes et robustes ?

Le cloisonnement est mis en œuvre à plusieurs niveaux techniques, suivant les types de ressources informatiques :

- Au niveau des **ressources de calcul ou de traitement** : les applications d'une zone sont exécutées sur des serveurs physiques, des machines virtuelles, ou des conteneurs, chacun apportant un niveau de cloisonnement différent et parfois complémentaire en fonction de leur mise en œuvre.

- Au niveau du réseau : le **réseau** peut être cloisonné en sous-réseaux, et une zone de sécurité peut être associée à un ou plusieurs sous-réseaux. Les mécanismes de cloisonnement réseau qui peuvent être mis en œuvre apportent différents niveaux de cloisonnement : commutateurs distincts d'une part, VLAN, VXLAN, Overlay, IPsec, OpenVPN, MACsec, d'autre part.

- Au niveau du **stockage** : en utilisant par exemple des disques ou des baies de disques dédiés à une zone, ou bien en associant à une zone un espace logique dans une baie ou un ensemble de serveurs mutualisés, ou encore en utilisant le chiffrement.

Parmi les moyens techniques ébauchés, on peut distinguer deux catégories, ceux qui mettent en œuvre un cloisonnement physique d'une part ou un cloisonnement logique d'autre part :

- Le **cloisonnement est dit « physique »** quand les ressources dédiées à une zone sont des équipements physiques, tels que des serveurs, des commutateurs ou des baies de stockage. Chaque équipement n'est utilisé que pour une zone.

- Le **cloisonnement est dit « logique »** quand les ressources associées à une zone partagent un équipement physique avec les ressources associées à d'autres zones. Par exemple, un hyperviseur hébergeant des machines virtuelles appartenant à des zones différentes.

Il est essentiel de considérer les différences en matière de risques et de niveaux de sécurité des modes de cloisonnements physique et logique – qui peuvent être complémentaires – et le niveau de sécurité apporté par chaque technologie. Il convient donc d'analyser ces modes et technologies au cas par cas, au-delà des considérations génériques décrites dans ce document.

Par ailleurs, il est essentiel qu'une zone de sécurité contienne des éléments ayant non seulement les mêmes besoins de sécurité (confidentialité, intégrité et disponibilité), mais également la même exposition et la même sensibilité.

S'il s'avère qu'un ou des éléments nécessitent une attention plus particulière, il est peut-être opportun de les cloisonner dans un sous-système.

Enfin, les zones, une fois définies et cloisonnées, doivent souvent être en interaction avec d'autres zones pour échanger des informations. Le point de contact entre deux zones est une **interconnexion**.

Modes de cloisonnement

Cette section présente quelques principes fondamentaux qui guident la conception, le choix et la mise en œuvre des mécanismes de cloisonnement au sein d'un système d'information.

Le cloisonnement d'une ressource au sein d'un SI doit être pensé en tenant compte de différents paramètres, tels que l'exposition, la sensibilité et les utilisateurs de cette ressource. Sans cette réflexion, le cloisonnement mis en œuvre peut manquer de robustesse et permettre à un attaquant de compromettre la ressource et de se latéraliser sur l'ensemble du système d'information.

Chaque ressource (calcul, réseau, stockage) peut être cloisonnée selon des modes de cloisonnement physique ou logique. Il faut bien prendre en compte les différences entre ces modes, mais aussi leur complémentarité.

Le cloisonnement physique assure une étanchéité par la séparation matérielle des équipements, tandis que le cloisonnement logique crée une isolation virtuelle par configuration logicielle au sein d'une infrastructure mutualisée.

Là où un mode de cloisonnement physique élimine le risque de latéralisation d'un attaquant, le cloisonnement logique, lui, l'atténue seulement. En effet l'introduction d'un élément logiciel permettant la mise en œuvre d'un cloisonnement logique implique nécessairement une augmentation de la surface d'attaque et de nouvelles vulnérabilités potentielles.

AVERTISSEMENT #1

Si la gestion des identités et des accès (voir fiche « ReCyF en pratique - Gestion des identités ») est parfois utilisée comme un moyen de cloisonnement logique, elle n'est pas considérée comme une thématique « d'architecture ». Elle ne peut en aucun cas se substituer au cloisonnement des ressources d'infrastructure pour, par exemple, couvrir les risques de latéralisation d'une attaque. C'est pourquoi elle n'est pas traitée ici.

AVERTISSEMENT #2

Lors de l'utilisation de cloisonnement logique, la sécurité de l'administration des mécanismes de cloisonnement est primordiale pour garantir leur bon fonctionnement et éviter leur détournement. Ainsi l'administration doit être au minimum au même niveau que la sensibilité de la ressource la plus critique et des contrôles doivent être mis en œuvre pour repérer toute erreur de configuration.

CLOISONNEMENT DES RESSOURCES DE CALCUL

CLOISONNEMENT PHYSIQUE

Le premier mode de cloisonnement des ressources de calcul repose sur la séparation physique des systèmes, applications et traitements, en les faisant fonctionner sur des serveurs matériels distincts. Le ou les serveurs sont dédiés aux calculs d'une zone de sécurité, et ne sont pas utilisés pour des calculs d'autres zones de sécurité.

Il s'agit donc d'un cloisonnement fondé sur le matériel : chaque zone de sécurité dispose de ses propres serveurs, avec ses composants (CPU, RAM, stockage, interfaces réseau), ce qui empêche toute interaction directe non maîtrisée avec les autres zones de sécurité.

Le cloisonnement physique est considéré comme le mode le plus robuste. Néanmoins, il reste impératif d'appliquer des mesures de durcissement, afin de renforcer leur niveau de sécurité.

→ *Voir la fiche « ReCyF en pratique – Durcissement et sécurité des équipements ».*

CLOISONNEMENT LOGIQUE AVEC MACHINES VIRTUELLES

Le mode de cloisonnement logique par machines virtuelles repose sur la virtualisation matérielle. Les ressources de calcul d'une zone de sécurité sont exécutées dans des machines virtuelles, sur un ou plusieurs serveurs matériels partagés : ces serveurs exécutent aussi des machines virtuelles d'autres zones de sécurité.

Ce partage de matériel est mis en œuvre par un hyperviseur. Un hyperviseur est un logiciel de virtualisation (ex. : ESXi, KVM, Xen, Hyper-V) qui permet d'exécuter plusieurs machines virtuelles indépendantes sur un même matériel physique. L'hyperviseur abstrait et partage les ressources matérielles (processeur, mémoire, stockage, réseau) tout en assurant une isolation entre les machines virtuelles. Ainsi, la compromission d'une application ou d'un traitement pouvant entrainer la compromission du système sera tout de même limitée au niveau de la machine virtuelle.

De manière générale, le cloisonnement par machines virtuelles est considéré comme le mécanisme logique le plus robuste. Cependant la compromission d'un hyperviseur par la compromission d'une machine virtuelle reste possible. Il reste donc recommandé de mutualiser sur un même hyperviseur des machines virtuelles de niveaux de sécurité homogènes (au sens décrit au chapitre des concepts), notamment lorsque les hyperviseurs sont regroupés en grappes (*clusters*).

CLOISONNEMENT LOGIQUE AVEC CONTENEURS

Le cloisonnement par conteneurs consiste à utiliser des technologies de conteneurisation telles que Docker ou Podman (avec ou sans technologies d'orchestration telles que Kubernetes) afin d'isoler des traitements au sein d'un même système d'exploitation hôte (qu'il s'agisse d'un serveur physique ou d'une machine virtuelle).

L'usage de conteneurs facilite les développements et les opérations. Du point de vue de la sécurité, ils permettent une séparation des binaires et librairies utilisés par l'application. Plusieurs mécanismes du noyau (*kernel*), correctement mis en œuvre sur un ensemble de conteneurs, peuvent limiter la surface d'attaque d'un conteneur vis-à-vis des autres.

Néanmoins les conteneurs partageant le même noyau (*kernel*) que l'hôte, la compromission d'un seul conteneur peut entraîner celle de l'hôte, et donc de l'ensemble des conteneurs exécutés sur celui-ci. Le cloisonnement logique avec conteneurs est donc un cloisonnement logique de niveau faible.

Aussi lorsque l'usage de conteneurs augmente au sein d'une entité, leur gestion peut nécessiter la mise en œuvre d'un orchestrateur. Un orchestrateur de conteneurs est un logiciel qui déploie, organise et supervise automatiquement les conteneurs et les applications exécutées dans ces derniers. Il gère la répartition de charge, le démarrage et l'arrêt des conteneurs, leur redémarrage en cas de panne et les communications réseau entre eux. L'ensemble de machines et conteneurs gérés par un même orchestrateur est là aussi appelé « grappe » (*cluster*).

À titre d'exemple, un orchestrateur comme Kubernetes permet d'exploiter des applications conteneurisées de manière fiable, évolutive et automatisée, sans gestion manuelle des conteneurs. Si l'introduction d'un orchestrateur permet une amélioration de la gestion opérationnelle des environnements, il est important de noter que celle-ci introduit certaines vulnérabilités pouvant encore augmenter la surface d'attaque des SI. Par exemple, lorsqu'une nouvelle vulnérabilité porte sur l'orchestrateur lui-même.

In fine il n'est pas recommandé de mutualiser sur un même hôte, ou sur une même *grappe* orchestrée, l'exécution de conteneurs de niveaux de sécurité hétérogènes.

CLOISONNEMENT DU RÉSEAU

CLOISONNEMENT PHYSIQUE

Ce mode de cloisonnement réseau repose sur la séparation des systèmes, applications et traitements en les faisant communiquer sur des matériels physiques dédiés : chaque zone dispose de ses propres matériels (ex. : commutateurs, routeurs, pare-feux) assurant un cloisonnement strict. Les interconnexions entre les zones, lorsqu'elles sont nécessaires, sont assurées par des pare-feux à cheval entre les zones.

Ce cloisonnement physique est considéré comme le mode le plus robuste. Néanmoins il reste impératif d'appliquer des mesures de durcissement aux équipements réseau, afin de sécuriser leur configuration.

CLOISONNEMENT LOGIQUE AVEC VIRTUALISATION

Le cloisonnement logique peut intervenir à différents niveaux du « modèle OSI[1] ».

Au niveau « liaison », le cloisonnement par virtualisation peut, par exemple, désigner l'emploi de réseaux locaux virtuels ou VLAN (*Virtual Local Area Network*). Cette technologie permet de créer plusieurs réseaux logiques sur un même équipement physique (commutateur), d'isoler les domaines de diffusion et de contrôler quels équipements peuvent communiquer entre eux.

Au niveau « réseau », il peut par exemple désigner l'emploi de VRF (*Virtual Route Forwarding*). Il s'agit d'une technique de cloisonnement logique consistant à faire coexister plusieurs tables de routage totalement indépendantes sur un même routeur.

Même si elles ne sont pas au niveau d'un cloisonnement par l'usage d'équipements physiques dédiés, ces technologies de cloisonnement logique sont aujourd'hui considérées comme robustes pour la plupart des niveaux de sécurité recherchés. Une attention particulière doit néanmoins être portée aux configurations sécurisées et à leur maintien dans le temps.

CLOISONNEMENT AVEC CHIFFREMENT

Le chiffrement des flux porte deux propriétés intéressantes. Il permet à la fois la protection des échanges en confidentialité, mais il permet aussi le cloisonnement des flux de l'extérieur, indépendamment du niveau de maîtrise et de confiance des équipements et réseaux traversés.

À titre d'exemples, le chiffrement des flux peut se faire au niveau du réseau avec la mise en œuvre d'un tunnel utilisant le protocole IPsec (*Internet Protocol Security*) ou au niveau applicatif à l'aide du protocole TLS (*Transport Layer Security*).

Configuré et maintenu suivant les *« Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques »*, le chiffrement permet d'obtenir un niveau de cloisonnement quasiment identique à un cloisonnement physique.

Il est important de noter que, si IPSec et TLS permettent effectivement de créer des réseaux privés virtuels (VPN) sécurisés et chiffrés, le chiffrement n'est pas pour autant une fonctionnalité implicite de tous les VPN. Par ex. GRE (*Generic Routing Encapsulation*, MPLS (*Multi Protocol Label Switching*) VPN, etc.

[1] Le modèle OSI (Open Systems Interconnection) est une norme de communication des systèmes informatiques en réseau. Ce modèle proposé par l'ISO (Organisation internationale de normalisation) décrit les fonctions nécessaires à la communication entre équipements informatiques ainsi que l'organisation de ces fonctions en couches superposées.

CLOISONNEMENT DU STOCKAGE

CLOISONNEMENT PHYSIQUE

Ce mode de cloisonnement du stockage repose sur la séparation des données sur des matériels physiques dédiés : chaque zone dispose de ses propres matériels (ex. : serveurs de stockage, NAS, systèmes SAN) assurant un cloisonnement strict.

Ce cloisonnement physique est considéré comme le mode le plus robuste. Néanmoins il reste impératif d'appliquer des mesures de durcissement aux équipements, afin de sécuriser leur configuration.

CLOISONNEMENT LOGIQUE

Le cloisonnement logique au niveau du stockage consiste à isoler virtuellement les flux et les données de différents utilisateurs ou systèmes au sein d'une même infrastructure physique de stockage, en utilisant des mécanismes logiciels (ex. : LUN, volumes) pour créer des frontières étanches.

L'efficacité de ce type de cloisonnement doit s'appuyer sur le principe de moindre privilège, sur une authentification forte pour l'administration des ressources de stockage et sur une politique stricte de mise à jour des logiciels mettant en œuvre ces mécanismes de cloisonnement logique.

CLOISONNEMENT AVEC CHIFFREMENT

Tout comme pour le réseau, le chiffrement des données stockées suivant les « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » permet d'obtenir un niveau de cloisonnement quasiment identique à un cloisonnement physique.

Il est néanmoins indispensable de rester vigilant aux moyens de génération et de gestion des secrets mis en œuvre pour ce chiffrement, ainsi qu'à la séparation des tâches entre les équipes de gestion du stockage et de gestion des clés.

AVERTISSEMENT #3

Dans un but de défense en profondeur, le chiffrement des flux réseau ainsi que des données stockées reste une pratique recommandée, quel que soit le mode de cloisonnement physique ou logique choisi.

Cloisonnement périmétrique

Il est nécessaire de cloisonner l'ensemble des systèmes d'information de l'entité vis-à-vis des systèmes tiers (ex. : Internet, prestataires, partenaires).

Si l'entité a exclu certains de ses SI de l'application des objectifs de sécurité réglementaires sur certains de ses SI, alors ces SI exclus doivent être considérés comme à l'extérieur du SI protégé, et donc à l'extérieur du cloisonnement périmétrique.

L'objectif est d'éviter qu'un incident de sécurité sur un système externe puisse se propager aux systèmes internes de l'entité. Ce cloisonnement peut être logique ou physique, mais doit être adapté : voir la section sur les modes de cloisonnement ci-dessus.

Cloisonnement interne

Chaque SI de l'entité doit être cloisonné des autres, même s'ils appartiennent à la même entité.

Cela évite qu'un incident sur un système impacte d'autres systèmes. Le cloisonnement peut être logique (réseaux distincts) ou physique (matériels séparés), y compris vis-à-vis de systèmes internes exemptés.

Pour chaque système d'information, l'entité doit se poser la question suivante : est-il pertinent de le découper en sous-systèmes ? Un sous-système regroupe des ressources ayant des fonctions similaires et un niveau comparable de sensibilité, d'exposition et de sécurité. Cette réflexion est obligatoire, même si elle aboutit à ne créer aucun sous-système. Dans ce cas, l'entité doit être capable de justifier ce choix (par exemple : système simple, peu exposé, avec des données homogènes, etc.).

Lorsque des sous-systèmes ont été définis, ils doivent être cloisonnés les uns des autres, là encore de manière logique ou physique. Le but est de limiter les conséquences d'un incident à un périmètre restreint. Ainsi, si un sous-système est compromis, les autres restent théoriquement protégés.

Cloisonnement de l'administration

Le découpage en zones du SI doit se refléter dans le cloisonnement des moyens d'administration.

En effet, le but premier est de protéger le SI d'administration de toute tentative de compromission du fait des privilèges élevés vers le SI administré. Un second objectif est de protéger le SI administré des intrusions et compromissions pour lesquelles le SI d'administration serait un vecteur d'attaque.

→ *Le sujet de l'administration fait l'objet de la fiche « ReCyF en pratique – Administration ».*

[2] IaaS : Infrastructure as a service
Infrastructure en tant que service

[3] PaaS : Platform as a service
Plate-forme en tant que service

[4] SaaS : Software as a service
Logiciel en tant que service

Cloisonnement dans un service cloud

Afin de faciliter la prise de décision dans les usages de l'informatique en nuage (ou cloud) selon la sensibilité des données et traitements d'une entité. Il est recommandé de consulter les *« Recommandations pour l'hébergement dans le cloud des systèmes d'information sensibles »* de l'ANSSI.

Les modalités de cloisonnement des ressources dans un service cloud dépendent d'une multitude de facteurs :

- les choix techniques du prestataire de service *cloud*, qui peut utiliser différents modes de cloisonnement entre ses services, entre ses clients ;
- le type de service, et donc le modèle de responsabilité associé (IaaS[2], PaaS[3], SaaS[4],...), car le choix des modes de cloisonnement des ressources (calcul, réseau, stockage) peut aussi être porté par le client et non plus par le prestataire.

La responsabilité du cloisonnement est partagée entre le prestataire cloud et le client, et doit être organisée selon le modèle de responsabilité :

- En IaaS, le prestataire cloisonne l'infrastructure physique entre clients, mais le cloisonnement entre machines virtuelles, systèmes, sous-systèmes et flux internes relève entièrement du client.
- En PaaS, le fournisseur prend en charge une partie du cloisonnement, mais le client reste parfois responsable des échanges et du découpage fonctionnel.
- En SaaS, le cloisonnement est majoritairement assuré par le prestataire, notamment entre clients.

En pratique, la bonne méthode consiste à identifier le modèle de responsabilité, à comprendre le niveau de cloisonnement associé au catalogue de services du prestataire, à déterminer ce qui reste sous la responsabilité du client, et le cas échéant à mettre en œuvre le cloisonnement complémentaire lorsque celui-ci est possible. Dans le cas contraire, l'entité doit assumer l'entière responsabilité des risques résiduels de la solution *cloud* retenue vis-à-vis de l'objectif de sécurité.

Une attention particulière doit être portée sur les solutions SaaS, dont le cloisonnement est majoritairement assuré par le prestataire. La qualification SecNumCloud pour les offres SaaS garantit les bonnes pratiques d'administration et un cloisonnement en adéquation avec le type de services rendus et les scénarios de menaces de l'éditeur.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FILTRAGE

Mesures ReCyF

Objectif de sécurité 7
Sécurisation de l'architecture des systèmes d'information
- Filtrage des communications : 7.B.1-EI/EE, 7.B.2-EE, 7.B.3-EI/EE, 7.B.4-EI/EE, 7.B.5-EI/EE

Le filtrage a pour but de garantir que les communications entre les différents systèmes et services de l'entité soient strictement maîtrisées. Dans un SI, les données circulent en permanence entre des serveurs, des applications, que ce soit en interne ou en externe de l'entité, en général à travers des réseaux informatiques. Si ces communications ne sont pas contrôlées, elles peuvent être détournées pour des attaques ou permettre des fuites de données.

On peut comparer un SI à un ensemble de bâtiments reliés par des routes. Chaque communication emprunte une route. Si toutes les routes sont ouvertes sans contrôle, n'importe qui peut circuler librement, y compris des personnes malveillantes. Pour limiter la circulation des personnes malveillantes, on doit identifier exactement quelles routes sont nécessaires, fermer toutes les autres et vérifier régulièrement que les routes ouvertes sont toujours justifiées.

En appliquant cette démarche, l'entité réduit significativement les risques d'intrusion, de propagation d'attaques et de fuite de données, tout en améliorant la compréhension et la maîtrise de son système d'information.

Identification et documentation des communications

La première étape consiste à identifier précisément les communications nécessaires au fonctionnement des activités de l'entité et au maintien de la sécurité de ses systèmes.

Cela concerne aussi bien les échanges entre les systèmes internes que les échanges avec des systèmes externes, comme ceux de prestataires ou de partenaires.

Chaque communication doit être décrite de manière claire et compréhensible. Il doit être possible de savoir quel système communique avec quel autre système, pour quelle raison et de quelle façon. Cette description permet d'avoir une vision globale et maîtrisée des échanges informatiques.

Lorsque l'entité a identifié des systèmes et des sous-systèmes (voir la section « Cloisonnement »), la description des communications doit être réalisée au niveau des sous-systèmes.

Cette démarche est essentielle, car une communication non identifiée est souvent une communication mal contrôlée. Elle peut rester ouverte sans raison valable et être exploitée à l'insu de l'entité. Par exemple, un serveur peut conserver un accès réseau mis en place pour un ancien usage et qui n'est plus nécessaire. Un attaquant pourrait alors utiliser cet accès oublié pour pénétrer dans le système.

Un exemple simple est celui d'un logiciel de paie qui doit transmettre des données à un prestataire externe une fois par mois. Cette communication est légitime et doit être documentée. En revanche, si le même serveur peut communiquer librement avec n'importe quel système externe sans justification, cela constitue un risque inutile.

Blocage par défaut des communications

De nombreuses attaques exploitent des canaux de communication qui n'auraient jamais dû être accessibles.

En bloquant tout ce qui n'est pas explicitement autorisé, on réduit fortement la surface d'attaque et on limite les possibilités d'exploitation, et donc de latéralisation.

En conséquence, une fois les communications nécessaires identifiées et documentées, seules celles-ci doivent être autorisées. Toutes les autres communications doivent être bloquées par défaut.

Filtrage des communications par des pare-feux

Un pare-feu est un dispositif qui contrôle les communications entre deux réseaux au niveau de leur interconnexion et décide, selon des règles définies, quelles communications sont autorisées ou bloquées.

Leur utilisation permet de centraliser les règles de filtrage et de mieux maîtriser les flux. Sans ces dispositifs, chaque système devrait gérer seul sa propre sécurité, ce qui augmente le risque d'erreurs et rend le contrôle global beaucoup plus complexe.

Les communications entre les différents systèmes de l'entité, ainsi qu'entre ceux-ci et les systèmes tiers, doivent être filtrées à l'aide de pare-feux. Ce filtrage périmétrique doit être réalisé à l'aide de pare-feux dédiés à cette fonction, distincts des pare-feux réalisant le filtrage interne. Cette mesure est justifiée par leur forte exposition et l'application du principe de défense en profondeur.

À titre d'exemple, un pare-feu mis en œuvre entre le réseau interne et Internet permet d'autoriser uniquement les services sortants nécessaires, comme l'accès au Web, tout en bloquant automatiquement les tentatives d'accès non prévues.

Revue régulière des règles de filtrage

Les systèmes d'information évoluent avec le temps : nouveaux outils, suppression ou création de systèmes ou plateformes, changement de prestataires, etc. Pour cette raison, les règles de filtrage sont évolutives.

L'entité doit donc effectuer **au moins une fois par an** une revue de la mise en œuvre technique des règles de filtrage. Cette revue permet de vérifier que les communications autorisées sont toujours nécessaires et que les règles sont correctement implémentées.

Sans cette vérification régulière, des règles obsolètes peuvent persister. Par exemple, un prestataire qui n'intervient plus depuis longtemps peut conserver des accès réseau toujours actifs. Ces accès oubliés constituent des failles potentielles, car ils peuvent être exploités par des personnes non autorisées.

Interconnexions – passerelles entrantes et sortantes

Chaque SI interagit avec d'autres systèmes d'information pour rendre un service ou pour son maintien en condition opérationnelle et de sécurité.

L'échange entre ces systèmes nécessite l'emploi de passerelles qui garantissent disponibilité, intégrité et confidentialité.

Il est nécessaire de faire la distinction entre les passerelles prenant en charge les communications sortantes et celles pour les communications entrantes. En effet, les risques sont différents selon le sens des flux. Les connexions sortantes doivent surtout être authentifiées et permettre de se prémunir de la fuite de données internes de l'entité. Les risques sur les communications entrantes portent davantage sur la compromission du SI interne.

Ainsi les SI de l'entité ne doivent pas se connecter directement aux systèmes externes. Toutes les connexions vers l'extérieur doivent passer par un point de passage contrôlé, appelé « passerelle sortante ». Cette passerelle sert à vérifier l'identité des utilisateurs ou des systèmes, à autoriser uniquement les connexions nécessaires et à garder une trace des accès réalisés.

Lorsque des systèmes externes doivent accéder à certaines ressources internes de l'entité, cet accès ne doit pas être direct. Il doit obligatoirement passer par une « passerelle entrante ». Cette passerelle doit permettre de limiter ce qui est accessible, de filtrer les connexions autorisées et de tracer les accès réalisés depuis l'extérieur ou depuis des systèmes internes exemptés, donc hors du périmètre considéré ici. L'objectif est de protéger les systèmes internes en exposant uniquement ce qui est strictement nécessaire.

Une interconnexion entre le SI et l'extérieur (Internet ou SI tiers) ne doit exister que si elle est réellement nécessaire. Les interconnexions doivent être justifiées soit par le fonctionnement normal des activités de l'entité, soit par des besoins techniques de maintenance ou de sécurité. Cela évite la multiplication de liens inutiles qui augmentent les risques en cas d'incident.

Cette approche d'interconnexion strictement nécessaire s'applique aussi entre sous-systèmes des entités ayant divisé leur système d'information.

ACCÈS DISTANTS

Mesures ReCyF

Objectif de sécurité 8
Sécurisation des accès distants aux systèmes d'information
- 8.1-EI/EE, 8.2-EI/EE, 8.3-EE, 8.4-EE, 8.5-EE

L'objectif est de protéger les accès distants aux systèmes d'information lorsque les flux transitent sur des réseaux ou des environnements qui ne sont pas directement maîtrisés par l'entité. Dès qu'un accès transite par un système tiers, par Internet ou depuis un lieu extérieur, les risques augmentent fortement : interception des communications, usurpation d'identité ou encore compromission de comptes.

Les mesures décrites ci-dessous visent à garantir la confidentialité des échanges à travers ces accès distants ainsi que l'identification et l'authentification des personnes. Pour cela, elles combinent trois principes essentiels : la confidentialité et l'intégrité des échanges grâce au chiffrement, la vérification de l'identité des utilisateurs par l'authentification multifacteur, et la protection des équipements utilisés hors des locaux de l'entité.

En appliquant ces mesures, l'entité réduit fortement les risques d'interception, d'usurpation d'identité et de compromission des terminaux, qui sont parmi les menaces les plus courantes liées aux accès à distance.

Protection des communications par le chiffrement

Lorsqu'un accès à un SI s'effectue à travers un système tiers, les communications doivent être protégées par des mécanismes de chiffrement conformes aux *« Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques »*.

Si elle le peut, l'entité tient compte des risques associés à la menace post-quantique (cf. *avis de l'ANSSI* et fiches techniques sur la transition des protocoles).
Le chiffrement permet de rendre les données illisibles. Même si un attaquant parvient à intercepter la communication, il ne pourra pas comprendre les informations échangées ni les modifier de manière exploitable.

Cette protection est indispensable lorsque les échanges transitent par Internet ou par des réseaux sur lesquels l'entité n'a aucun contrôle direct. Des technologies comme les réseaux privés virtuels (VPN) chiffrés ou les protocoles applicatifs chiffrés permettent de créer un canal sécurisé entre l'utilisateur et le système cible.

Par exemple, un utilisateur qui se connecte à distance à une application interne depuis son domicile fait transiter des informations sensibles sur Internet. Sans chiffrement, ces données pourraient être interceptées ou altérées. Avec un chiffrement adapté, les informations restent protégées tout au long de leur parcours.

Authentification des accès de l'entité ou de ses prestataires

En plus de la protection des communications, il est essentiel de vérifier de manière fiable l'identité et les droits d'accès de la personne ou du service qui se connecte, qu'il s'agisse d'un utilisateur interne ou d'un prestataire mandaté.

Un mécanisme d'authentification conforme aux règles de sécurité de la fiche « Gestion des identités et des accès » doit donc être mis en œuvre. L'objectif est d'éviter qu'une personne non autorisée puisse se faire passer pour un collaborateur, un service ou un prestataire légitime, même si elle connaît un identifiant et un mot de passe.

Sans authentification robuste, un attaquant ayant récupéré des authentifiants (ex. : un identifiant et un mot de passe) par hameçonnage ou par fuite de données pourrait accéder aux systèmes comme s'il était un utilisateur autorisé.

Pour renforcer la sécurité des accès distants, le mécanisme d'authentification doit être multifacteur et reposer au minimum sur un facteur dit « de connaissance », comme un code secret.

L'authentification multifacteur consiste à combiner plusieurs éléments (facteurs) d'authentification de nature différente afin de valider l'identité d'un utilisateur. Il peut s'agir, par exemple, de quelque chose que l'on connaît (un code), de quelque chose que l'on possède (une carte ou un téléphone) ou de quelque chose que l'on est (une caractéristique biométrique). Cette combinaison rend les attaques beaucoup plus difficiles, car même si un attaquant parvient à obtenir un premier facteur, il ne pourra pas se connecter sans disposer du second.

→ *Le sujet de la gestion des identités fait l'objet de la fiche « ReCyF en pratique – Gestion des identités ».*

Dans certaines situations, des contraintes techniques ou opérationnelles peuvent empêcher la mise en œuvre d'une authentification multifacteur. Ces cas doivent rester exceptionnels et être justifiés.

Le cas échéant, l'entité doit mettre en place des mesures alternatives permettant de réduire le risque. L'objectif est alors de compenser l'absence de facteurs multiples par d'autres protections. Par exemple, il peut s'agir de limiter strictement les plages horaires de connexion, de restreindre les adresses réseau autorisées, de renforcer la surveillance des accès ou d'appliquer des contrôles supplémentaires sur les actions possibles une fois connecté.

Protection des postes de travail et équipements mobiles

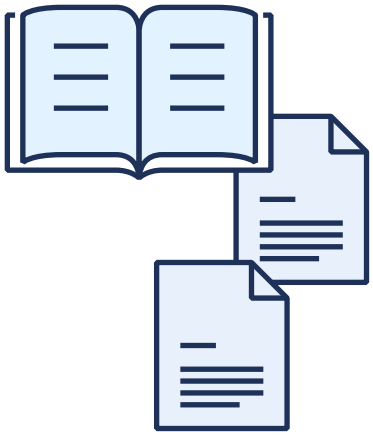
Les postes de travail et les équipements mobiles utilisés pour accéder à distance aux systèmes d'information présentent un risque particulier car ils peuvent être utilisés depuis des lieux non maîtrisés par l'entité, et être perdus ou volés.

Les mémoires de masse de ces équipements, comme les disques de stockage, doivent donc être protégées en permanence par des mécanismes de chiffrement et d'authentification conformes à l'état de l'art.

Le chiffrement des disques (ex. : Bitlocker, LUKS, Cryhod) permet d'appliquer un haut niveau de protection des données stockées en cas de vol ou de perte de l'équipement. L'authentification au démarrage empêche une personne non autorisée d'accéder aux informations simplement en allumant l'appareil.

ANNEXES

Annexe 1: bibliographie



Documents ANSSI

- Référentiel Cyber France
Consulter le lien

- Les essentiels – Architecture sécurisée de SI
Consulter le lien

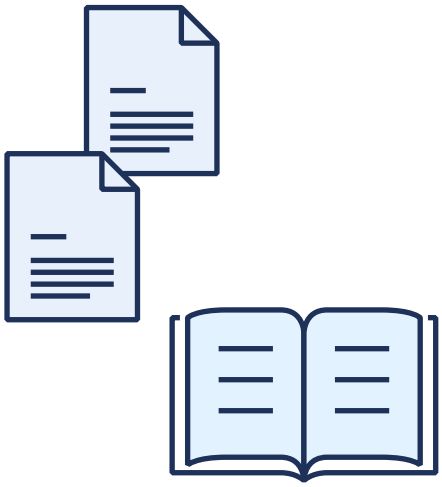
- Les essentiels – Virtualisation
Consulter le lien

- Guide d'hygiène informatique
Consulter le lien

- Recommandations pour la protection des systèmes d'information essentiels
Consulter le lien

- Recommandations pour l'hébergement dans le cloud des systèmes d'information sensibles
Consulter le lien

- Référentiel d'exigences SecNumCloud v3.2
Consulter le lien



- Recommandations relatives à l'interconnexion d'un système d'information à Internet
Consulter le lien

- Recommandations relatives à l'authentification multifacteur et aux mots de passe
Consulter le lien

- Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques
Consulter le lien

- Recommandations sur le nomadisme numérique
Consulter le lien

- Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique et fiches techniques sur la transition des protocoles
Consulter le lien

Annexe 2 : extrait du glossaire ReCyF

Mesures ReCyF	Définition
Action d'administration	Installation, suppression, modification ou consultation d'une configuration d'une ressource d'un système d'information susceptible de modifier le fonctionnement ou la sécurité de celui-ci.
Administrateur	Personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration ou de maintenance sur celui-ci, responsable d'un ou plusieurs domaines techniques.
Annuaire	Ressource logicielle centralisant des informations relatives aux utilisateurs, et parfois aux autres ressources d'un système d'information et fournissant des mécanismes d'identification et d'authentification. *Par exemple : Microsoft Active Directory, OpenLDAP.*
Information sensible	Les données à caractère personnel « sensibles » au sens du 1 de l'article 9 du Règlement (UE) 2016/679, les données d'une sensibilité particulière au titre de l'article 31 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, les données protégées au titre de l'article L. 151-1 du code de commerce ainsi que les données protégées au titre de la protection du patrimoine scientifique et technologique de la nation
Interconnexion	Ressource logicielle ou matérielle rendant possible le transfert d'information entre deux systèmes d'information ou entre deux sous-systèmes par une continuité de signaux électromagnétiques (par exemple : câble réseau, diode optique).
Règle de filtrage	Instruction implémentée au sein d'un dispositif de filtrage (par exemple : un pare-feu) visant à autoriser ou interdire les flux de données en fonction : ▸ De l'adresse IP source ou destination ; ▸ Du protocole utilisé par le flux de données (*par exemple : TCP ou UDP*) ; ▸ Des numéros de port source ou destination (*par exemple : TCP/23*) ▸ De l'applicatif.
Réseau	Ensemble de ressources interconnectées permettant de communiquer au sein d'un ou plusieurs systèmes d'information
Réseau d'administration	Réseau dédié physiquement ou logiquement aux flux internes à ce réseau et les flux d'administration vers les systèmes d'information
Sous-système	Ensemble de composants d'un système d'informations constitués pour assurer une fonctionnalité ou un ensemble homogène de fonctionnalités d'un système d'information ou encore pour isoler des ressources d'un système d'information ayant un même besoin de sécurité.
Système d'information	Ensemble des infrastructures et services logiciels informatiques relevant de la responsabilité de l'entité, permettant de collecter, traiter, transmettre et stocker sous forme numérique les données. Les ressources informatiques partagées ou mutualisées avec des tiers relevant du périmètre de responsabilité de l'entité, sont considérées comme faisant partie intégrante des systèmes d'information de l'entité, et sont à ce titre pleinement assujetties aux obligations de la directive NIS 2.
Système d'information d'infrastructure	Système d'information généraliste utile aux activités ou aux services de l'entité, ou nécessaire au fonctionnement de plusieurs systèmes d'information de l'entité. *Par exemple : annuaire, messagerie, téléphonie, service de résolution de nom de domaine.* Un système d'information d'infrastructure peut être un système d'information.
Systèmes d'information tiers	Système d'information ou ressource informatique partagée ou mutualisée avec l'entité qui n'est pas sous la responsabilité de l'entité. *Point d'attention : lorsque l'entité externalise tout ou partie de son système d'information, ce dernier reste sous sa responsabilité et n'est donc considéré comme un SI tiers au sens du présent référentiel.*
Utilisateur	Personnels de l'entité et prestataires agissant pour le compte de l'entité qui accèdent aux systèmes d'information.