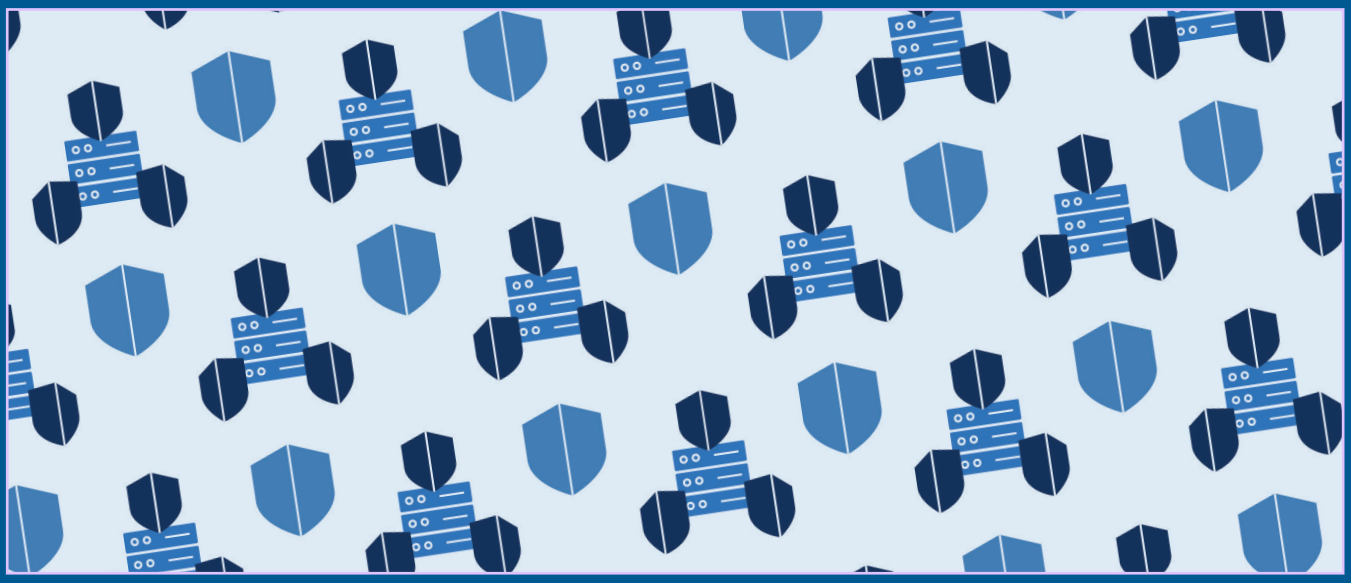


Durcissement et sécurité des équipements

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'entité se protège des codes malveillants qui pourraient être introduits sur ses systèmes d'information.

Elle restreint la connexion de ressources matérielles à ses systèmes d'information, qui répond exclusivement à des besoins justifiés et en lien avec ses activités.

Elle s'assure que seules les ressources logicielles strictement nécessaires sont installées ou conservées sur ses systèmes d'information. Elle en maintient une configuration sécurisée et robuste (principe de durcissement) pour réduire les risques d'attaques exploitant des vulnérabilités ou des faiblesses de configuration.

Approche générale



CONTEXTE

Codes malveillants

Les codes malveillants sont des programmes informatiques ou des fichiers conçus pour nuire à des équipements informatiques.

Ils peuvent également nuire à des systèmes d'information dans leur ensemble lorsqu'ils ont des capacités de propagation automatique (infection d'autres équipements informatiques par le réseau ou les périphériques connectés). Les codes malveillants peuvent par exemple être des virus, des rançongiciels, des programmes ou scripts d'attaque utilisés par des attaquants.

Les préjudices causés par les codes malveillants dépendent de leur sophistication et de la motivation des attaquants. Le plus souvent, ces préjudices incluent :

- La mise hors service ou en état de fonctionnement dégradé des équipements informatiques et industriels de l'entité : mise à l'arrêt d'une chaîne de production industrielle par remise à zéro des équipements qui la pilotent, altération de systèmes de sûreté pouvant causer des accidents, introduction de défauts volontaires dans des processus de fabrication, etc. ;
- L'indisponibilité ou la fuite de données : leur vol dans le cadre d'un espionnage industriel et commercial ou pour leur vente au plus offrant, leur confiscation contre rançon, etc. Ce vol est généralement réalisé via l'utilisation de rançongiciels qui chiffrent les données et ne les restituent qu'après le paiement d'une rançon en cryptomonnaies (aussi appelées cybermonnaies) ;
- L'utilisation frauduleuse des ressources informatiques de l'entité : minage de cryptomonnaies[1], lancement d'attaques informatiques vers des systèmes d'information tiers, etc. ;
- Le détournement de fonds : virements et transactions bancaires frauduleux à l'insu de l'entité, vol de cryptomonnaies, etc.

[1] L'utilisation de la puissance de calcul des systèmes entraîne leur ralentissement et une consommation électrique élevée, ce qui se traduit notamment par un préjudice économique.

Équipements informatiques

Les équipements informatiques qui présentent des risques d'exécution et de propagation de codes malveillants sont, de manière générale, tout équipement exécutant un système d'exploitation, aussi léger soit-il.

Les équipements informatiques les plus importants pour une entité sont généralement les serveurs et les postes de travail, ainsi que les différents équipements industriels. Les recommandations de sécurité abordées dans le présent document sont donc essentiellement orientées vers la sécurisation de ces équipements. Néanmoins, les risques d'exécution et de propagation de codes malveillants concernent aussi plus largement :

- Les *smartphones*, tablettes, montres connectées et autres appareils intelligents de la vie quotidienne ;
- Les routeurs réseau, points d'accès Wi-Fi, concentrateurs et autres équipements de l'infrastructure réseau ;
- Les équipements de sûreté (les caméras notamment).

Périphériques

Les périphériques (claviers, clés USB, casques audio, etc.) ne sont pas autonomes et n'ont généralement d'utilité qu'une fois connectés aux équipements informatiques.

À la différence de ces derniers, les périphériques sont généralement limités dans leur capacité à exécuter des opérations autres que celles pour lesquelles ils ont été conçus. Ils peuvent malgré tout propager des codes malveillants de différentes manières :

- Passivement, en stockant des codes malveillants qu'un utilisateur est susceptible d'exécuter lui-même sur un ou plusieurs équipements informatiques. C'est par exemple le cas d'une clé USB qui contiendrait un virus ;
- Activement, en déclenchant automatiquement des actions, voire de l'exécution de code, sur les équipements informatiques auxquels ils sont connectés. C'est par exemple le cas d'un matériel connecté par USB, y compris supposément pour sa seule recharge électrique (cigarette électronique par exemple), mais qui, à l'insu de l'utilisateur, se comporterait en réalité comme un clavier pour exécuter des instructions malveillantes sur l'équipement informatique.

Ces périphériques potentiellement dangereux sont généralement connectés aux équipements informatiques par USB, voire par appairage Bluetooth. En étant connectés aux équipements informatiques, il est admis que ces périphériques sont indirectement connectés aux systèmes d'information de l'entité. Ils peuvent donc y propager des codes malveillants.

Besoin de sécurisation

Étant donné les risques qui pèsent sur les équipements informatiques et les périphériques en termes d'actions et de codes malveillants, il est primordial que l'entité se protège de manière adéquate.

Cette protection repose sur deux axes :

- Maîtriser la connexion de matériel aux systèmes d'information, pour éviter la propagation des codes malveillants (voir section *« Politique de connexion aux systèmes d'information »*) ;
- Déployer des solutions de sécurité ayant pour finalité de protéger les équipements informatiques contre l'exécution de codes malveillants (voir section *« Solutions de protection contre les codes malveillants »*.)

POLITIQUE DE CONNEXION AUX SYSTÈMES D'INFORMATION

Mesures ReCyF

Objectif de sécurité 9
Protection des systèmes d'information contre les codes malveillants
- 9.1-EI/EE, 9.2-EE, 9.5-EI/EE

Politique de connexion des équipements informatiques

La connexion d'un équipement informatique à un système d'information de l'entité lui permet d'interagir avec d'autres équipements informatiques qui y sont également connectés.

Elle s'effectue généralement par l'intermédiaire d'un réseau filaire (par câble réseau : RJ45, fibre optique, etc.) ou sans-fil (Wi-Fi) pour permettre à l'équipement d'accéder à des ressources informatiques (services métier, données, accès Internet, etc.). Toute connexion représente donc un risque potentiel de propagation de codes malveillants. Pour cette raison, il est primordial que l'entité définisse et mette en œuvre une politique en matière de connexion d'équipements informatiques à ses systèmes d'information. Cette politique consiste à simplement déterminer ce qui est autorisé ou interdit, en fonction de critères qu'elle précise. Des critères d'autorisation que l'entité peut retenir sont par exemple :

- La nature de l'équipement informatique : poste de travail, serveur, smartphone, tablette, routeur réseau, point d'accès Wi-Fi, etc. ;
- Le propriétaire de l'équipement informatique : l'entité elle-même, un prestataire, un salarié, un visiteur, etc. ;
- Des conditions techniques et organisationnelles : ancienneté maximale des mises à jour, présence de solutions logicielles de sécurité (cf. section « Solutions de protection contre les codes malveillants »), etc. ;
- Les emplacements de connexion autorisés : locaux de l'entité, salles serveur, locaux techniques de brassage réseau, salles de réunion, espaces visiteurs, lieux de télétravail autorisés, etc.

Pour aller plus loin, une telle politique devrait également limiter les autorisations de connexion aux seuls besoins justifiés et en lien avec les activités de l'entité. Ces restrictions de connexion sont développées dans la section « Restrictions de connexion des ressources matérielles ».

Politique de connexion des périphériques

La même démarche est à suivre pour les périphériques, quelle que soit leur nature.

Les concernant, des critères d'autorisation que l'entité peut retenir sont notamment :

- La nature du périphérique : clé USB, casque audio USB, clavier sans fil, etc. ;
- Le propriétaire du périphérique : l'entité elle-même, un prestataire, un salarié, un visiteur, etc. ;
- Sa provenance : acquis par l'entité, fourni par un prestataire, acheté par un salarié, objet publicitaire, provenance inconnue, etc. ;
- Les équipements actifs auxquels la connexion du périphérique est autorisée : serveurs, postes de travail, postes de développement logiciel, poste de recherche et développement, postes d'administration, etc.

Parmi les périphériques, les supports amovibles réinscriptibles[2] sont ceux qui font courir le plus de risques de propagation de codes malveillants. Ils doivent faire l'objet d'une attention particulière, développée dans la section « Restrictions de connexion des supports de stockage amovibles ».

Pour aller plus loin, ces restrictions devraient être étendues à tous types de périphériques ; elles sont développées dans la section « Restrictions de connexion des ressources matérielles ».

[2] Un support amovible réinscriptible est un périphérique de stockage de données sur lequel il est possible de lire et écrire à plusieurs reprises. Les supports amovibles réinscriptibles les plus répandus sont les clés USB et les disques durs portables USB.

Restrictions de connexion des supports de stockage amovibles réinscriptibles

Les supports de stockage amovibles réinscriptibles (principalement les clés USB et disques durs USB) sont susceptibles de contenir, intentionnellement ou non, des fichiers malveillants et de les propager dans les systèmes d'information de l'entité.

Il est donc particulièrement important d'en limiter l'usage à travers les politiques de connexion définies par l'entité. Pour remplir cet objectif, toute connexion de supports de stockage amovibles devrait exclusivement répondre à un besoin légitime en lien avec les activités de l'entité :

- La réalisation de ses missions et la fourniture de ses services : disque dur USB utilisé pour le transport de fichiers métier entre deux systèmes d'information, clé USB de livraison d'une commande de composant logiciel, clé USB d'un auditeur comptable, etc.

- Le maintien en condition opérationnelle ou de sécurité (MCO/MCS) de ses systèmes d'information : clés USB nécessaires au déploiement de systèmes et de logiciels hors-ligne, clés USB de dépannage informatique, etc.

Restrictions de connexion des ressources matérielles

Pour un niveau de sécurité accru, la restriction de connexion des supports de stockage amovibles réinscriptibles décrite précédemment est un principe qu'il est nécessaire d'étendre à toutes les ressources matérielles de l'entité, c'est-à-dire à tous les équipements informatiques ainsi qu'à tous types de périphériques.

Leur connexion devrait ainsi répondre exclusivement à un besoin légitime en lien avec les activités de l'entité (réalisation de ses missions, fourniture de ses services, maintien en condition opérationnelle et de sécurité de ses systèmes d'information). Les ressources matérielles autorisées par l'entité peuvent par exemple être intégrées au sein de :

- Ses systèmes d'information industriels : les systèmes de télégestion des installations industrielles (serveurs SCADA et stations de travail opérateur notamment), les automates, etc. ;

- Ses systèmes d'information de bureautique : les postes de travail qui lui appartiennent, les claviers et souris fournis avec ces équipements, les casques audio, webcams et microphones acquis par l'entité pour la visioconférence, les clés USB acquises et étiquetées par l'entité, etc. ;

- Ses systèmes d'information dédiés à l'administration informatique : ses postes et serveurs d'administration, les ressources informatiques qui leur sont dédiées, etc. ;

- Ses salles serveur uniquement : l'infrastructure de maintien en conditions opérationnelles et de sécurité de ses systèmes d'information. Elle se compose par exemple des infrastructures de sauvegarde des données, infrastructures de messagerie électronique, serveurs de gestion centralisée des configurations et de déploiement des mises à jour, serveurs de supervision de la sécurité des systèmes d'information, etc.

D'autre part, l'entité est uniquement en mesure d'estimer le niveau de sécurité des ressources matérielles qu'elle maîtrise. Il est ainsi pertinent d'autoriser uniquement la connexion à ses systèmes d'information :

- Des ressources matérielles qui appartiennent à l'entité et qu'elle gère elle-même ;
- Des ressources matérielles qui sont gérées par des prestataires qu'elle a expressément mandatés pour cette mission (c'est-à-dire les prestataires avec lesquels l'entité a signé un contrat de sous-traitance de leur gestion). Dans ce cas, les contrats qui lient l'entité à ces prestataires définissent clairement les obligations de sécurité qui leur sont applicables dans le cadre de cette gestion sous-traitée.

À l'inverse, dans le cadre d'une politique BYOD (*bring your own device*), aussi nommée AVEC (*apportez votre équipement personnel de communication*) en français, un équipement informatique personnel est géré par l'utilisateur lui-même, puisqu'il en est le propriétaire. L'entité n'a aucun moyen de connaître son niveau de sécurité. Il est ainsi préférable d'interdire la connexion d'équipements personnels (ordinateurs et smartphones notamment) aux systèmes d'information d'une entité. Il en va de même pour les périphériques : une clé USB trouvée sur un parking ou donnée sur un stand dans un salon est susceptible de contenir, intentionnellement ou non, des fichiers malveillants, voire de réaliser des actions malveillantes à l'insu de l'utilisateur. Pour cette raison, il est préférable d'interdire la connexion d'équipements informatiques et de périphériques USB qui n'ont pas été acquis par l'entité elle-même ou par ses partenaires.

Réseau dédié aux équipements interdits

Pour les équipements informatiques qu'elle interdit dans ses systèmes d'information, une entité a la possibilité de déployer des réseaux qui leur sont dédiés.

Ces réseaux spécifiques doivent uniquement permettre un accès restreint à des ressources informatiques qui peuvent être compromises sans aucun préjudice pour l'entité. C'est par exemple le cas d'un réseau Wi-Fi dédié aux visiteurs et aux équipements informatiques personnels (réseau souvent appelé « réseau visiteur »), offrant uniquement une connectivité Internet.

Pour que ces réseaux visiteurs soient considérés distincts des systèmes d'information de l'entité, ils doivent être strictement isolés, tant sur le plan réseau que sur celui de leurs équipements informatiques. Cette isolation, préférablement faite par cloisonnement physique (concept décrit dans la fiche « ReCyF en pratique - Architecture sécurisée »), est nécessaire pour garantir que d'éventuelles menaces présentes dans ces réseaux visiteurs ne puissent pas se propager vers les autres systèmes d'information.



MESURES DE SÉCURITÉ D'APPLICATION DES POLITIQUES DE CONNEXION

Mesures ReCyF

Objectif de sécurité 9
Protection des systèmes d'information contre les codes malveillants
- 9.3-EI/EE, 9.4-EE, 9.5-EI/EE

L'efficacité des politiques citées dans les sections précédentes est conditionnée à la mise en œuvre de mesures de sécurité organisationnelles ou techniques, idéalement complémentaires.

Les mesures de sécurité organisationnelles reposent sur la compréhension, l'adhésion et la discipline des utilisateurs. Leur efficacité dépend donc de la capacité de l'entité à formaliser ses règles de sécurité, puis à informer et sensibiliser ses collaborateurs. À cette fin, l'entité peut par exemple formaliser ses règles de sécurité dans une charte informatique. Elle peut également utiliser différents canaux de communication oraux ou écrits, ponctuels ou réguliers : sessions de sensibilisation, campagnes de courriels, affiches, etc. Des contrôles périodiques peuvent également être réalisés pour vérifier la bonne compréhension et l'application effective des règles.

Les mesures de sécurité techniques sont, au contraire, automatisées et systématiques. Elles offrent une protection plus robuste car elles ne dépendent pas des utilisateurs, mais leur mise en œuvre peut s'avérer plus complexe. Des mesures de sécurité techniques peuvent être appliquées par l'entité pour empêcher la connexion d'équipements informatiques et de périphériques non autorisés à ses systèmes d'information. Ces mesures permettent notamment de :

- S'assurer que seuls les équipements autorisés obtiennent une connectivité sur les réseaux des systèmes d'information. De la sorte, brancher un équipement à une prise réseau ne donne aucun accès réseau tant que l'équipement n'est pas autorisé par l'infrastructure réseau. Différentes solutions de contrôle d'accès réseau (filaire ou sans fil) peuvent être mises en œuvre à cet effet. Plusieurs mesures de sécurité possibles sont détaillées dans le cas pratique « Contrôle d'accès réseau » ;

- Authentifier, lorsque le contrôle d'accès réseau n'est pas possible (cas de réseaux en accès libre pour des raisons opérationnelles ou organisationnelles), les flux réseau préalablement à toute possibilité de communication avec les ressources informatiques des systèmes d'information. En général, cela se traduit par une connexion obligatoire à un VPN (*virtual private network*) d'entreprise (avec, de préférence, une authentification multifacteurs). Dans ce cas-là, le VPN doit être basé sur un protocole effectuant du chiffrement, comme par exemple IPsec, WireGuard ou OpenVPN. Les ressources informatiques des systèmes d'information sont ainsi positionnées derrière les serveurs VPN et ne sont accessibles qu'à travers eux. Le *guide de l'ANSSI sur le nomadisme numérique* est une lecture recommandée pour appréhender le fonctionnement des accès VPN et prendre connaissance des recommandations de mise en œuvre sécurisée ;

- Contrôler finement, à défaut de contrôle d'accès réseau et de VPN obligatoire, l'accès physique aux locaux (ce sujet est approfondi dans le cas pratique « Contrôle d'accès physique aux locaux »). Si cela concerne un réseau Wi-Fi, il convient également de vérifier que la portée de son signal n'excède pas le périmètre des locaux faisant l'objet d'un contrôlé d'accès physique ;

- Mettre en œuvre des restrictions logicielles sur la connexion de périphériques aux équipements informatiques. Elles sont présentées dans le cas pratique « Contrôle des périphériques amovibles ».

SOLUTIONS DE PROTECTION CONTRE LES CODES MALVEILLANTS

Mesures ReCyF

Objectif de sécurité 9
Protection des systèmes d'information contre les codes malveillants
- 9.6-EI/EE, 9.7-EI/EE

Objectif de sécurité 5
Maîtrise des systèmes d'information
- Maintien en condition opérationnelle et de sécurité : 5.B.2-EI/EE

Les équipements informatiques connectés aux systèmes d'information de l'entité sont susceptibles d'exécuter du code malveillant chaque fois qu'ils traitent du contenu provenant de sources externes (d'Internet, de partenaires, d'équipements informatiques personnels, entre autres), quel que soit son format.

Par principe, tout contenu provenant de sources externes doit être considéré comme potentiellement malveillant. Le contenu potentiellement malveillant peut ainsi provenir :

- D'Internet, notamment via :
  - → La navigation Web, dans la mesure où les pages Web visitées peuvent cacher du code malveillant exécuté par le navigateur au moment de la visite ;
  - → La messagerie électronique (c'est-à-dire le contenu de la boîte mail, qu'elle soit accessible en ligne via un navigateur Web ou à l'aide d'un logiciel dédié), sachant que les courriels reçus peuvent contenir des liens vers du contenu malveillant, des pièces jointes malveillantes, voire directement du code malveillant potentiellement exécuté par le client de messagerie dès l'ouverture d'un message ;
  - → Les échanges de fichiers entre l'entité et ses clients ou partenaires, quelle que soit la solution de transport de l'information utilisée, étant donné que ces fichiers peuvent contenir du code malveillant.
- De périphériques connectés aux systèmes d'information de l'entité, notamment les supports amovibles réinscriptibles, qui peuvent stocker des codes malveillants provenant de sources externes.

En règle générale, le code malveillant s'exécute à l'insu de l'utilisateur et de manière invisible, c'est-à-dire sans que rien ne puisse alerter l'utilisateur.

Protection des équipements informatiques contre les codes malveillants

Dans la grande majorité des cas, les missions d'une entité sont principalement assurées à l'aide d'équipements informatiques qui peuvent être exposés à du contenu potentiellement malveillant.

Dès lors, il est important que ceux connectés aux systèmes d'information de l'entité soient protégés par des mécanismes de protection contre les codes malveillants. Ces mécanismes peuvent notamment remplir les fonctions suivantes :

- Contrôler l'innocuité[3] de tout contenu avant son traitement, de sorte à le bloquer ou le supprimer de manière préventive ;
- Détecter le comportement potentiellement malveillant d'un code en cours d'exécution, puis de l'interrompre le cas échéant ;
- Restreindre la connexion de périphériques, en bloquant ceux qui ne sont pas autorisés ;
- Contrôler les flux réseau pour détecter et bloquer des tentatives de propagation de codes malveillants ou d'attaques menées depuis d'autres équipements informatiques du système d'information ;
- Détecter des indicateurs de compromission, c'est-à-dire une combinaison d'informations techniques et contextuelles représentatives de l'exécution d'un code malveillant.

Les solutions de sécurité du commerce qui portent une partie ou l'ensemble de ces fonctions de sécurité sont notamment :

- Les antivirus, qui font principalement du contrôle d'innocuité de contenu reposant sur des bases de données de signatures de contenus connus pour être malveillants ;
- Les EDR (*endpoint detection and response*), qui détectent principalement des comportements potentiellement malveillants ou des indicateurs de compromission, puis appliquent automatiquement des contre-mesures (isolation réseau de l'équipement par exemple) pour éviter une propagation de code malveillant ;
- Les EPP (*endpoint protection platform*), qui sont des solutions de sécurité cumulant une fonctionnalité d'antivirus et des fonctionnalités additionnelles telles que : l'analyse comportementale, la restriction de connexion des périphériques, l'analyse et le contrôle des flux réseau, etc.

En complément, il est utile de préciser que :

- Plusieurs solutions de sécurité peuvent éventuellement être déployées sur un même équipement informatique, dans l'objectif d'agréger des fonctions de sécurité distinctes et complémentaires (par exemple : un antivirus et un agent EDR sur un même équipement). Dans ce cas, il est conseillé de s'assurer préalablement de leur compatibilité mutuelle (par exemple, la présence de deux solutions de sécurité ayant une ou plusieurs fonctions de sécurité identiques activées sur un même équipement est souvent source de dysfonctionnements) ;
- Varier les solutions de sécurité mises en œuvre au sein d'un système d'information peut avoir du sens pour réduire les risques liés à la défaillance de l'une d'elles. Ce sujet est détaillé dans le cas pratique « Varier les solutions de sécurité » ;
- Certains types d'équipements restent encore trop peu souvent protégés par des solutions de sécurité. C'est notamment le cas des équipements informatiques utilisés dans les milieux industriels, tels que les systèmes de télégestion des installations industrielles. Le *guide de l'ANSSI sur la cybersécurité des systèmes industriels* traite notamment des menaces les concernant et explique comment les protéger.

[3] L'innocuité d'un contenu signifie que ce dernier n'est pas malveillant. À noter que l'innocuité ne peut jamais être garantie puisque les solutions de protection contre les codes malveillants n'ont pas un taux de détection de 100 % des menaces.

Protection périmetrique des systèmes d'information contre les codes malveillants

Il convient de s'assurer que les contenus provenant de sources externes, donc potentiellement malveillants, fassent l'objet d'une analyse automatique lors de leur entrée dans les systèmes d'information.

Dans ce but, l'entité déploie des solutions de sécurité ayant pour fonction de contrôler l'innocuité du contenu sur les équipements informatiques ayant un rôle de porte d'entrée du système d'information. C'est notamment le rôle :

- Des passerelles de messagerie, qui analysent les courriels et les pièces jointes reçus avant leur distribution aux utilisateurs ;
- Des serveurs mandataires (proxy), qui sont des serveurs placés en intermédiaires des flux réseau. Ils analysent par exemple les flux de navigation Web et les fichiers téléchargés ;
- Des sas de décontamination (également appelés « stations blanches »), qui ont vocation à être les seuls équipements informatiques auxquels la connexion de supports de stockage amovibles réinscriptibles non maîtrisés est autorisée. Ils décontaminent les données dans leur transit entre les supports amovibles et les systèmes d'information. Étant donné que ces équipements particuliers sont fortement exposés aux codes malveillants, ils sont généralement conçus et sécurisés spécifiquement pour ce cas d'usage, dans l'objectif de les rendre robustes face aux risques d'exécution de code malveillant.

Exceptions possibles à l'analyse de sécurité d'un contenu

Dans quelques rares cas, un contenu provenant de sources externes pourrait ne pas faire l'objet d'une analyse de sécurité lors de son entrée dans les systèmes d'information de l'entité.

Pour qu'une telle exception soit autorisée, il est fortement recommandé que ce contenu satisfasse au minimum à ces trois conditions :

1. Il provient de partenaires que l'entité estime fiables (fournisseurs reconnus de logiciels, prestataires liés par un contrat, etc.) et rigoureux quant à la sécurité de leurs systèmes d'information.

2. Son origine et son intégrité sont garanties techniquement, par exemple au moyen d'une signature électronique. Une vérification de signature permet de garantir que le contenu est bien l'original et qu'il n'a pas été modifié. Les hash (ou condensats en français) vérifient, quant à eux, uniquement l'intégrité d'un fichier.

3. L'analyse de son innocuité lors de son entrée dans le SI n'est pas possible ou n'est pas pertinente du fait de contraintes techniques particulières.

Ces rares exceptions à l'analyse antivirale concernent, le plus souvent, un type de contenu bien particulier : des programmes ou mises à jour fournis par certains éditeurs. C'est par exemple le cas répandu des mises à jour et correctifs de sécurité Windows fournies par Microsoft. En règle générale, les programmes informatiques distribués par les éditeurs sont signés. Sous Windows par exemple, la fonctionnalité « *Microsoft Defender SmartScreen* » permet de vérifier la signature des fichiers exécutables (d'exécution de logiciels ou d'installation de logiciels) avant leur exécution, et affiche un message d'avertissement à l'utilisateur si la signature est incorrecte (si le fichier n'est pas original ou s'il a été modifié). Pour ces rares exceptions, la vérification de la signature tient lieu d'analyse.

Attention toutefois : tous les contenus restent exposés, à la source, à des attaques de la chaîne d'approvisionnement dont le degré de vraisemblance et les impacts doivent être évalués par l'entité.

Exceptions possibles à la protection d'un équipement contre les codes malveillants

Dans quelques rares cas, des équipements informatiques spécifiques (du fait de leur isolement ou de leur usage particulièrement contrôlé) peuvent éventuellement être dépourvus de mécanismes de protection contre les risques d'exécution de codes malveillants.

Pour qu'une telle exception soit autorisée, il est fortement recommandé que ces équipements informatiques spécifiques satisfassent au minimum ces cinq conditions :

1. Ils ne traitent que de contenu signé électroniquement et dont l'innocuité a été préalablement vérifiée dans les systèmes d'information de l'entité (sauf exceptions détaillées en section « Exceptions possibles à l'analyse antivirale d'un contenu »).

2. Il est jugé que l'installation d'une solution de protection contre les codes malveillants sur ces équipements présente un mauvais rapport bénéfice/risque.

3. Seuls des périphériques de confiance peuvent y être connectés.

4. Ils sont situés dans des locaux dont l'accès physique est restreint, réservé à du personnel en lequel l'entité a suffisamment confiance (personnel habilité ou accrédité par exemple).

5. Ils sont administrés et gérés par du personnel en lequel l'entité a particulièrement confiance (les équipes d'administration informatique par exemple).

De tels équipements informatiques sont par exemple :

- Les serveurs « contrôleurs de domaine *Active Directory* » (ces serveurs particuliers sont détaillés dans la fiche « ReCyF en pratique – Gestion des utilisateurs ») et ceux du cœur de confiance du SI de manière générale (concept détaillé dans la fiche « ReCyF en pratique – Administration »)
- Les serveurs WSUS (*Windows Server Update Services*) de distribution de mises à jour et de correctifs de sécurité aux systèmes Windows, entre autres.

Attention toutefois : ces exceptions ne sont pas définitives. Il est pertinent de les réévaluer en tenant notamment compte de l'évolution des menaces ou des recommandations des éditeurs et de l'Autorité nationale de sécurité des systèmes d'information.

Mise à jour des solutions de protection contre les codes malveillants

Pour préserver leur capacité de protection dans le temps, les solutions de sécurité mises en œuvre par l'entité à des fins de protection contre les codes malveillants nécessitent d'être tenues à jour (version logicielle, version des moteurs d'analyse, signatures, indicateurs de compromission, etc.).

Le sujet du maintien en conditions opérationnelle et de sécurité est davantage détaillé dans l'objectif de sécurité ReCyF n° 5 « Maîtrise des systèmes d'information ».

LOGICIELS INSTALLÉS SUR LES ÉQUIPEMENTS

Mesures ReCyF

Objectif de sécurité 18
Sécurisation de la configuration des ressources des systèmes d'information
- Configuration : 18.1-EE, 18.2-EE, 18.3-EE, 18.4-EE

Objectif de sécurité 5
Maîtrise des systèmes d'information
- Maintien en condition opérationnelle et de sécurité : 5.B.3-EI/EE, 5.B.4-EI/EE

Sur les équipements informatiques, les ressources logicielles sont multiples, parmi lesquelles :

- Les systèmes d'exploitation des équipements : Windows, Linux, etc. ;
- Les logiciels installés ou préinstallés : suite de bureautique, navigateur Web et ses extensions, client de messagerie, logiciel métier, antivirus, etc. ;
- Les dépendances logicielles tierces dont les équipements ont éventuellement besoin pour fonctionner : environnement d'exécution Java, *framework .NET*, etc. ;
- Les scripts et autres programmes dédiés à des tâches de gestion et d'administration des équipements informatiques : script d'inventaire logiciel, script de configuration, programme de migration applicative, etc. ;
- Les logiciels optionnels qui sont nativement présents dans les systèmes d'exploitation, notamment sous forme de services (applications exécutées en arrière-plan sans interface utilisateur, qui peuvent être automatiquement exécutées au démarrage de l'équipement, souvent avec des droits élevés) : service de collecte d'événements de journalisation, service de déport d'affichage à travers le réseau, etc. Il est à noter que les services ne peuvent pas toujours être désinstallés, mais ils peuvent généralement être désactivés.

Par le biais des logiciels présents sur les équipements informatiques, des codes malveillants sont susceptibles d'être introduits, de se propager et de s'exécuter dans les systèmes d'information de l'entité : lors de leur installation initiale, lors de leur mise à jour, ou via du contenu externe qu'eux-mêmes sont susceptibles de récupérer depuis Internet (modules complémentaires téléchargeables, par exemple).

Risques liés aux logiciels

Chaque logiciel est susceptible d'augmenter la surface d'attaque des équipements informatiques, voire des systèmes d'information dans leur ensemble.

Cette surface d'attaque représente leur degré d'exposition face aux cybermenaces, notamment au travers de leurs fonctionnalités de traitement de contenus dont les faiblesses peuvent être exploitées par du contenu malveillant.

Par exemple, un navigateur Web traite comme contenu des pages Web (entre autres). Ces pages Web sont potentiellement malveillantes puisque l'entité n'en maîtrise pas le contenu. Leur analyse et leur interprétation par le navigateur pour les retranscrire graphiquement sont des opérations complexes. Il est ainsi courant que des défauts dans les moteurs d'analyse et d'interprétation soient exploitables par un attaquant pour amener le navigateur à exécuter du code malveillant dissimulé dans ces pages. Des dizaines de nouvelles vulnérabilités sont découvertes chaque année dans les navigateurs, et elles sont souvent utilisées par des attaquants pour l'exécution de code malveillant. Les victimes l'exécutent à leur insu au moment de la navigation sur un site Web contenant une page malveillante, généralement sans en avoir conscience puisque l'exécution est souvent invisible.

La plupart des logiciels souffrent régulièrement de vulnérabilités exploitées par les attaquants. Ils sont par conséquent des portes d'entrée potentielles pour les codes malveillants dans les systèmes d'information de l'entité : clients de messagerie, suites de bureautique, lecteurs de fichiers PDF, lecteurs vidéo, visionneuses d'images, etc.

Restriction des logiciels

Étant donné les risques que représentent les logiciels pour un système d'information, leur présence sur les équipements informatiques de l'entité devrait répondre exclusivement à un besoin justifié, en lien avec les activités de l'entité.

Seuls devraient donc être autorisés le déploiement et la conservation de logiciels nécessaires à la réalisation de ses missions, à la fourniture de ses services ou au maintien en conditions opérationnelle et de sécurité.

Pour limiter et contrôler les logiciels présents sur les équipements informatiques connectés à ses systèmes d'information, l'entité peut par exemple s'assurer que :

- Seuls les administrateurs ont les droits (autorisations) nécessaires à l'installation de logiciels sur ces équipements ;
- Les logiciels autorisés sont directement intégrés dans les images de base (*masters*)[4] tenues à jour et destinées à l'installation initiale des équipements, ou bien que leur déploiement est piloté par une solution logicielle centralisée de télé-déploiement automatique ou à la demande de l'utilisateur via un catalogue d'applications maîtrisé par l'entité et interne au SI (également appelé magasin d'applications ou *application store*) ;
- Un inventaire logiciel, de préférence automatique, est régulièrement réalisé pour lister les logiciels présents sur ces équipements ;
- Les logiciels qui ne sont plus autorisés sont désinstallés ou désactivés, automatiquement ou manuellement.

Dans certains cas, des raisons techniques ou opérationnelles peuvent justifier qu'un logiciel inutile ne soit ni désinstallé ni désactivé (si cela fait perdre le support éditeur, par exemple). Dans ce cas, l'entité met en œuvre des mesures de sécurité pour réduire la probabilité que ce logiciel traite du contenu potentiellement malveillant. Les mesures de sécurité suivantes sont par exemple envisageables :

- En interdire techniquement l'exécution par des droits utilisateurs spécifiques ou par des mécanismes de restrictions logicielles (détaillés dans le cas pratique « Mécanismes de restrictions logicielles ») ;
- En bloquer l'accès réseau, par des règles de filtrage entrantes ou sortantes de pare-feux ;
- En interdire l'usage de manière organisationnelle, par le biais d'une charte informatique ou d'une PSSI par exemple.

Enfin, il peut arriver que des besoins spécifiques poussent les entités à fournir des équipements informatiques dédiés à ceux-ci (par exemple : des postes d'audit, de recherche ou de développement). Sur ces équipements, il est envisageable de permettre à l'utilisateur d'installer ou d'exécuter librement les logiciels qu'il considère nécessaires à son activité professionnelle, si les trois conditions suivantes sont réunies :

1. Ces besoins sont non-standards vis-à-vis des activités métier principales de l'entité.
2. Ces besoins ne concernent pas l'administration des systèmes d'information.
3. L'utilisateur a régulièrement besoin d'installer ou d'exécuter des logiciels, et a donc besoin d'une certaine autonomie.

Une telle autorisation fait l'objet d'un processus de validation au sein de l'entité, en précisant notamment le périmètre des permissions octroyées et leur durée. Dans le cas où l'utilisateur obtient la permission d'installer et d'exécuter des logiciels, il existe alors une forme de co-responsabilité :

- L'entité reste elle-même responsable de la sécurité et du durcissement de l'équipement informatique malgré une configuration permissive en termes de restrictions logicielles. Les solutions de sécurité peuvent, par exemple, bloquer l'installation d'un logiciel par l'utilisateur si ce logiciel est détecté comme malveillant ;

[4] L'installation de logiciels dans des images de base est généralement adaptée aux seuls logiciels qui sont communs à tous les équipements, ou quand ces images sont destinées à des équipements dépourvus de connectivité réseau. Le déploiement centralisé à travers le réseau reste la méthode à privilégier : elle simplifie le déploiement de versions à jour et permet un contrôle fin des périmètres de déploiement (pour les logiciels soumis à licences par exemple).

- L'utilisateur devient lui-aussi responsable des permissions qui lui sont octroyées. Ses responsabilités, ses obligations et le régime de sanctions sont dans ce cas précisés à l'utilisateur, qui ne doit pas les ignorer. L'entité le forme pour qu'il soit en mesure de remplir ses obligations en termes de sécurité des systèmes d'information et de vigilance numérique. Elle lui met notamment à disposition des interlocuteurs formés pour répondre à ses questions ou pour prendre en charge des signalements de sécurité numérique.

Les équipements informatiques sur lesquels les utilisateurs ont des permissions étendues présentent des risques de sécurité accrus. Ils ne devraient pas être sur le même réseau que les équipements standards, et leurs interactions avec les systèmes d'information devraient être réduites au minimum. Il est par exemple envisageable d'uniquement autoriser ces équipements non-standards à se connecter au réseau Wi-Fi visiteur.

En complément, l'entité s'assure que les politiques de sécurité de ses systèmes d'information et ses chartes numériques sont mises à jour en conséquence. Elle y clarifie ce partage de responsabilités et y décrit les mesures mises en œuvre pour traiter les risques de sécurité relatifs aux équipements sur lesquels des utilisateurs obtiennent des permissions étendues.

Configuration sécurisée des logiciels autorisés

Il convient de s'assurer que tous les logiciels présents dans les systèmes d'information de l'entité soient configurés de manière sécurisée.

Les configurations par défaut des logiciels étant généralement définies pour une compatibilité optimale, sans objectifs de sécurité, il est nécessaire d'apporter les changements de configuration requis pour leur sécurisation dès leur déploiement initial.

Pour cela, il est recommandé de s'appuyer sur les recommandations de configuration et de sécurisation des éditeurs (elles sont généralement documentées), des fabricants, ainsi que de l'Autorité nationale de sécurité des systèmes d'information (à travers les guides, les alertes de sécurité, etc.). La configuration sécurisée des équipements informatiques et des logiciels est abordée de manière plus détaillée dans le cas pratique « Configuration sécurisée des logiciels ».

Mise à jour des logiciels

Pour préserver leur niveau de sécurité, les logiciels présents dans les systèmes d'information doivent être tenus à jour via le déploiement de leurs derniers correctifs de sécurité.

Le sujet du maintien en conditions opérationnelles et de sécurité est davantage détaillé dans la fiche correspondante.

Maintien des configurations sécurisées

Les configurations sécurisées appliquées lors des déploiements initiaux doivent être maintenues dans le temps et rester pertinentes.

Par exemple, une mise à jour logicielle peut rendre un paramètre [5] de sécurité obsolète ou le remplacer par un autre, tout comme elle peut introduire de nouveaux paramètres dont la valeur par défaut engendre de nouveaux risques de sécurité. À cet égard, une revue régulière (au minimum annuelle) des configurations des logiciels présents dans les systèmes d'information est recommandée. Elle permet de vérifier que les configurations effectives restent conformes aux configurations sécurisées attendues, et que ces dernières sont toujours adaptées aux besoins de compatibilité et aux menaces, qui évoluent dans le temps. La revue des configurations des logiciels peut se faire en :

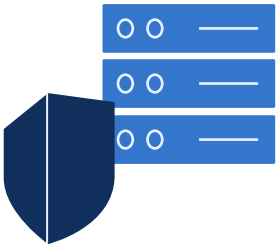
- Utilisant des outils de scans de vulnérabilités et de faiblesses logicielles ;
- Utilisant des outils de contrôle de conformité des systèmes, au regard des stratégies de sécurité définies par l'entité ;
- Analysant la pertinence des règles de filtrage appliquées par les logiciels de sécurité (justesse des exclusions antivirales, adéquation des règles de pare-feu vis-à-vis des matrices de flux réseau autorisés, etc.) ;
- Procédant à des audits de sécurité, en interne ou en recourant à des prestations de service spécialisées.

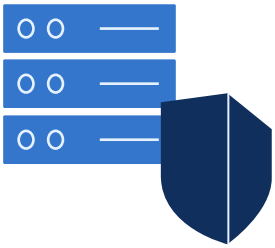
[5] Les notes de mise à jour publiées par les éditeurs informent généralement sur les nouvelles fonctionnalités ainsi que des évolutions des paramètres de configuration du logiciel. Leur lecture permet de savoir si la configuration du logiciel doit être revue.

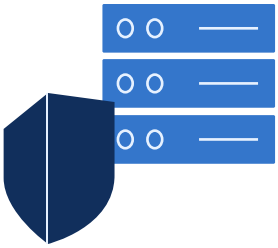


CAS PRATIQUES

Les cas pratiques présentés ci-dessous constituent des propositions illustrant diverses façons de mettre en œuvre les recommandations formulées.
Le lecteur est invité à retenir, selon son contexte et ses besoins, les éléments qui lui semblent les plus pertinents.

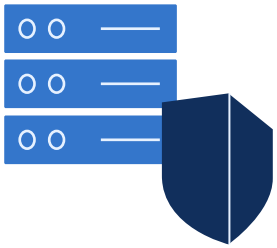






Contrôle d'accès réseau

Le contrôle d'accès réseau peut se faire de différentes manières. Celles évoquées ci-après sont les plus communément utilisées.



Méthodes communes aux réseaux filaires et Wi-Fi :

- Un contrôle d'accès réseau simple peut être mis en œuvre par filtrage MAC (adresse physique unique à chaque carte réseau) sur les équipements des infrastructures réseau (commutateurs, concentrateurs, etc.), ainsi que sur les points d'accès Wi-Fi. Un équipement informatique dont l'adresse MAC n'est pas autorisée se voit ainsi refuser l'accès au réseau. Cette mesure de sécurité présente l'avantage d'être compatible avec n'importe quel équipement, puisque tous ont obligatoirement une adresse MAC et qu'aucune configuration n'est nécessaire sur ces derniers : toute la configuration se fait au niveau de l'infrastructure réseau. En revanche, ce filtrage a une faiblesse : il peut être mis en défaut puisqu'il est trivial d'usurper une adresse MAC (cas d'un équipement informatique, contrôlé par un attaquant, se faisant passer pour un autre en falsifiant son adresse MAC). Par exemple, un attaquant peut débrancher une imprimante réseau, se brancher à sa place et utiliser son adresse MAC pour voler l'accès réseau de l'imprimante. Un contrôle d'accès plus robuste est donc conseillé si les besoins de sécurité de l'entité le justifient, et si les contraintes opérationnelles le permettent.

- Un contrôle d'accès réseau plus robuste peut être mis en l'œuvre à l'aide du protocole 802.1x, qui consiste en un contrôle d'accès de l'équipement par un secret qui peut être un mot de passe ou, idéalement, un certificat d'authentification. Les secrets doivent être déployés sur les équipements informatiques, et ces derniers les utilisent pour s'authentifier auprès de l'infrastructure réseau (plus précisément, c'est généralement un serveur RADIUS qui procède à l'authentification). L'utilisation de certificats est préférable à celle de mots de passe, dans la mesure où les certificats sont individuels (différents par équipement), que leurs stockages peuvent être sécurisés au niveau matériel (à l'aide d'un TPM (*Truster Platform Module*), par exemple) et qu'ils peuvent être révoqués lorsqu'un équipement est impacté par un incident de sécurité. Un équipement non muni d'un secret d'authentification valide (généralement parce qu'il n'est géré ni par l'entité, ni par un prestataire qu'elle a mandaté) se voit refuser l'accès au réseau, et donc au système d'information. *Un guide de l'ANSSI traite du déploiement sécurisé d'un contrôle d'accès réseau par utilisation du protocole 802.1X*.

Méthodes spécifiques aux réseaux Wi-Fi :

- Un contrôle d'accès réseau simple peut être mis en œuvre en sécurisant l'accès au réseau Wi-Fi par clé partagée (la clé étant une suite de caractères, comme un mot de passe). Une clé partagée d'accès Wi-Fi présente cependant plusieurs défauts :
  - → En règle générale, elle est connue des utilisateurs qui peuvent donc l'utiliser avec n'importe quel équipement, y compris ceux qui ne sont pas autorisés par l'entité ;
  - → En fonction de sa longueur et du paramétrage du réseau Wi-Fi, il existe des attaques automatisées permettant de la deviner par analyse des ondes électromagnétiques ;
  - → Elle n'est pas stockée de manière sécurisée sur les équipements informatiques, elle peut donc être volée ou divulguée ;
  - → Elle est commune à tous les équipements informatiques d'un même réseau Wi-Fi. Bien qu'il soit recommandé de la renouveler régulièrement, il s'agit d'une opération rarement réalisée étant donné la contrainte que cela représente.

- Un contrôle d'accès Wi-Fi par portail captif peut être utilisé pour demander quelques informations préalablement à l'ouverture de l'accès (par exemple : nom, société, adresse mail professionnelle).

- Il est important qu'un réseau Wi-Fi ne soit pas « ouvert » (accessible en libre accès par quiconque), sans quoi n'importe quel équipement informatique pourrait y être connecté. Des réseaux Wi-Fi ouverts acceptables d'un point de vue de la sécurité des systèmes d'information sont éventuellement :
  - → Les réseaux Wi-Fi dédiés aux visiteurs (cf. section « Réseau dédié aux équipements interdits »), bien que l'utilisation d'un portail captif soit à privilégier ;
  - → Les réseaux Wi-Fi depuis lesquels un VPN est ensuite obligatoire pour accéder à Internet ou aux ressources informatiques de l'entité (cf. section « Mesures de sécurité d'application de la politique de connexion »).

- Un contrôle d'accès réseau Wi-Fi robuste peut être mis en œuvre en reposant sur une authentification par certificats, ces derniers devant être préalablement délivrés aux équipements clients. L'authentification par certificat est rendue possible sur les points d'accès Wi-Fi à l'aide de protocoles tels que PEAP/EAP-TLS ou EAP-TLS. Un équipement non muni d'un certificat d'authentification valide (généralement parce qu'il n'est géré ni par l'entité, ni par un prestataire qu'elle a mandaté) se voit refuser l'accès au réseau Wi-Fi, et donc au système d'information. Il est ainsi préférable de mettre en œuvre une authentification par certificat plutôt qu'une authentification par clé d'accès Wi-Fi

À noter que certains équipements spécifiques, comme les équipements industriels, ne supportent pas ces fonctionnalités de contrôle d'accès. Parfois, il arrive également que des équipements soient trop critiques pour faire l'objet de quelconque changement de configuration ou d'interruption de service. Dans ces différents cas, le contrôle d'accès réseau peut au minimum reposer sur le filtrage des adresses MAC, ainsi que sur le contrôlé d'accès physique aux locaux (cf. le cas pratique « Contrôle d'accès physique aux locaux »).

Contrôle des périphériques amovibles

La restriction de connexion des périphériques est généralement possible de manière native sur les principaux systèmes d'exploitation à l'aide de listes d'autorisation et de listes d'interdiction.

Dans ces listes, un périphérique peut être identifié par son identifiant matériel, qui est principalement constitué d'un identifiant de fournisseur, ainsi que du nom et de la version du périphérique. Des identifiants génériques relatifs au type de matériel peuvent également être utilisés. À l'aide de ces listes, une entité a par exemple la possibilité de n'autoriser que la connexion USB de claviers, de souris et de certains modèles de périphériques amovibles réinscriptibles (généralement des clés USB et des disques durs portables). Cependant, la mise en œuvre et le suivi de ces restrictions nécessitent un certain effort à l'échelle d'un système d'information. Pour une mise en œuvre sous Windows, se référer à l'article correspondant qui figure dans la bibliographie.

Des solutions logicielles du commerce proposent également des fonctionnalités de restriction de connexion des périphériques. Elles se distinguent généralement par leur facilité de mise en œuvre et de gestion par rapport aux seuls mécanismes natifs du système d'exploitation. Il est à noter que de telles fonctionnalités sont parfois intégrées aux solutions logicielles de protection contre les codes malveillants. Pour les équipements informatiques sur lesquels la connexion de périphériques USB ou l'appairage *Bluetooth* sont complètement interdits, il est possible de désactiver ces ports dans la plupart des BIOS et UEFI.

Enfin, certains équipements spécifiques, comme les équipements industriels, ne sont pas dotés de fonctionnalités de restriction des périphériques amovibles, ou ces fonctionnalités ne sont pas activables. Dans ce cas, le contrôle d'accès physique aux locaux (cf. le cas pratique « Contrôle d'accès physique aux locaux ») est primordial pour réduire le risque de connexion de périphériques non autorisés sur ces équipements non protégés.

Mécanismes de restrictions logicielles

Des mécanismes de restrictions logicielles peuvent être mis en œuvre sur certains systèmes d'exploitation.

Sous Windows, par exemple, les trois principaux mécanismes natifs sont :

- SRP, obsolète et remplacé par *Applocker* ;
- *Applocker*, dont l'utilisation est à privilégier en raison de son bon compromis entre sécurité et facilité de mise en œuvre. Des articles de Microsoft et un guide de l'ANSSI documentent les étapes de mise en œuvre de ce mécanisme ;
- *Application Control for Windows* (ou *App Control for Business dans les environnements entreprise*), qui est plus efficace que les deux précédents, mais dont la mise en œuvre est la plus complexe. Il est également documenté par Microsoft.

Sous Linux, les mécanismes souvent utilisés sont *AppArmor*, *SELinux* et IMA (*Integrity Measurement Architecture*). Le *guide de l'ANSSI de sécurisation d'un système GNU/Linux* traite notamment de ces sujets.

En général, les mécanismes de restrictions logicielles permettent d'autoriser ou interdire des logiciels à l'aide de règles construites sur différents critères tels que :

- Le nom du logiciel (nom de l'exécutable, du script ou de la bibliothèque) ;
- Le chemin d'accès (local ou réseau) ;
- L'empreinte cryptographique (condensat) ;
- Les informations figurant dans la signature électronique (éditeur, nom, version, etc.) ;
- Les utilisateurs ou groupes d'utilisateurs auxquels s'appliquent l'autorisation ou l'interdiction.

Des solutions logicielles du commerce proposent également des fonctionnalités de restrictions logicielles. Elles se distinguent généralement par leur facilité de mise en œuvre et de gestion par rapport aux seuls mécanismes natifs du système d'exploitation. De telles fonctionnalités sont parfois intégrées aux solutions logicielles de protection contre les codes malveillants.

Enfin, certains équipements spécifiques, comme les équipements industriels, ne sont pas dotés de fonctionnalités de restrictions logicielles, ou ces fonctionnalités ne sont pas activables. Sur de tels équipements, il est primordial de réduire le risque d'exécution de codes malveillants en limitant les utilisateurs ayant des droits d'exécution de logiciels.

Contrôle d'accès physique aux locaux

Lorsque des réseaux sont dépourvus de contrôle d'accès réseau, une manière d'assurer la bonne application des règles d'autorisation de connexion des équipements informatiques est de positionner ces équipements dans des locaux dont l'accès physique est particulièrement restreint et supervisé (c'est-à-dire avec une traçabilité et une revue régulière des entrées de personnel).

C'est souvent le cas d'une salle serveur, dont l'accès physique est renforcé au regard de la criticité des équipements informatiques qui s'y trouvent. Le personnel des équipes d'administration informatique et réseau y entre par exemple à l'aide d'un badge d'accès nominatif non duplicable, et la badgeuse enregistre les traces de tous les accès réalisés. Des systèmes de contrôle d'accès alternatifs peuvent par exemple reposer sur un lecteur d'empreintes digitales, voire une simple clé dont l'utilisation est associée au remplissage d'un livre faisant office de registre d'accès. En parallèle, ces locaux peuvent faire l'objet d'une surveillance spécifique, par exemple à l'aide de caméras de surveillance.

Le plus souvent, il n'est pas primordial de déployer de mécanismes de contrôle d'accès réseau en salle serveur, à partir du moment où le contrôle est déporté sur la restriction d'accès physique au local (accès par badge nominatif par exemple) et sa surveillance. Pour plus de détails, le guide de l'ANSSI de sécurisation des systèmes de contrôle d'accès physique est une lecture recommandée. Ce sujet fait également l'objet de l'objectif de sécurité ReCyF n° 6 « maitrise des accès physiques aux locaux ».

Varier les solutions de sécurité

Les solutions de sécurité (antivirus, EDR, etc.) ne garantissent pas un taux de détection de 100 % des menaces.

Il est donc approprié de varier les solutions de sécurité mises en œuvre. Cette stratégie se traduit généralement par :

- Des solutions de sécurité distinctes sur les serveurs et les postes de travail. Pour être complémentaires, ces solutions utilisent des bases antivirales différentes ;

- Des solutions de sécurité différentes sur les équipements informatiques périmétriques du système d'information (sas de décontamination, passerelles de filtrage des courriels, serveurs mandataires Web, etc.). Dans une logique de complémentarité, les solutions de protection contre les codes malveillants dont ils sont munis ne sont pas les mêmes que sur le reste du système d'information.

Le choix de multiplier les solutions de sécurité doit se faire en garantissant la bonne maîtrise et la maintenance de celles-ci dans le temps, en particulier : leur maintien en condition de sécurité, leur bonne configuration, une gestion adaptée des alertes, etc.

Configuration sécurisée des logiciels

La configuration sécurisée des logiciels peut reposer sur de nombreuses ressources documentaires et techniques :

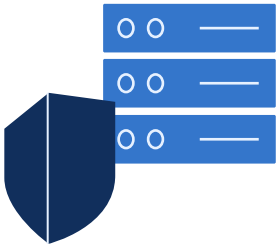
- Pour la sécurisation des systèmes d'exploitation Windows, Microsoft publie des lignes de base de sécurité (*baselines*) qui peuvent par exemple être appliquées sur les systèmes à l'aide des stratégies de groupe.

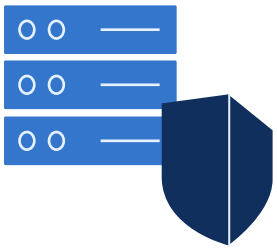
- Les éditeurs de logiciels et les fabricants de matériel spécifique documentent parfois les étapes à suivre pour leur configuration sécurisée, ou proposent des fichiers de configuration à appliquer.

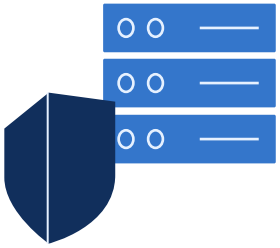
- L'ANSSI publie des recommandations de sécurisation spécifiques à des logiciels très utilisés, qui peuvent être suivies pour mettre en œuvre une configuration sécurisée. Dans tous les cas, il est conseillé d'en étudier la mise en œuvre, y compris en complément ou en remplacement des recommandations des éditeurs.

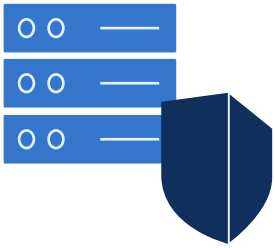
- Enfin, dans l'éventualité où aucune des sources précédentes ne propose de recommandations de sécurisation, des sources alternatives réputées peuvent être utilisées (STIGS, CIS, etc.). Dans ce cas, l'entité est invitée à adopter un esprit critique vis-à-vis des configurations proposées.

Attention : l'entité doit être particulièrement méfiante vis-à-vis de l'utilisation de configurations provenant de sources douteuses ou automatisées (proposées par des intelligences artificielles par exemple). Il est important de bien les analyser avant leur mise en œuvre.

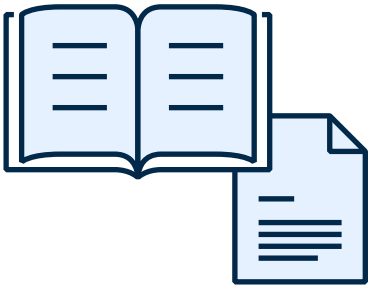








ANNEXES



Annexe 1: bibliographie

Documents ANSSI

- Référentiel Cyber France
Consulter le lien

- Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques
Consulter le lien

- La cybersécurité des systèmes industriels
Consulter le lien

- Mettre en œuvre une politique de restrictions logicielles sous Windows
Consulter le lien

- Recommandations de déploiement du protocole 802.1X
Consulter le lien

- Recommandations de sécurité relatives à un système GNU/Linux
Consulter le lien

- Recommandations sur le nomadisme numérique
Consulter le lien

- Sécurisation des systèmes de contrôle d'accès physique et vidéoprotection
Consulter le lien

- Sécuriser les accès Wi-Fi
Consulter le lien

Documents éditeurs

- Gestion des périphériques autorisés sous Windows
Consulter le lien

- Contrôle d'application pour Windows
Consulter le lien

Annexe 2 : extrait du glossaire ReCyF

Mesures ReCyF	Définition
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.*
Code malveillant	Tout ou partie d'un programme ou d'un fichier permettant d'utiliser une ou plusieurs vulnérabilités d'un logiciel (du système ou d'une application) à des fins malveillantes.
Cœur de confiance	Ensemble des ressources regroupant les annuaires, les ressources hébergeant ces annuaires ou permettant d'en prendre le contrôle.
Réseau	Ensemble de ressources interconnectées permettant de communiquer au sein d'un ou plusieurs systèmes d'information.
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 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.*
Utilisateurs	Personnels de l'entité et prestataires agissant pour le compte de l'entité qui accèdent aux systèmes d'information.