GUIDE D'HYGIÈNE INFORMATIQUE

RENFORCER LA SÉCURITÉ DE SON SYSTÈME D'INFORMATION EN 42 MESURES

AVANT-PROPOS

Paru en janvier 2013 dans sa première version, le Guide d'hygiène informatique édité par l'ANSSI s'adresse aux entités publiques ou privées dotées d'une direction des systèmes d'information (DSI) ou de professionnels dont la mission est de veiller à leur sécurité. Il est né du constat que si les mesures qui y sont édictées avaient été appliquées par les entités concernées, la majeure partie des attaques informatiques ayant requis une intervention de l'agence aurait pu être évitée.

Cette nouvelle version a fait l'objet d'une mise à jour portant à la fois sur les technologies et pratiques – nouvelles ou croissantes – avec lesquelles il s'agit de composer en matière de sécurité (nomadisme, séparation des usages, etc.) mais aussi sur la mise à disposition d'outils (indicateurs de niveau standard ou renforcé) pour éclairer le lecteur dans l'appréciation des mesures énoncées. Si l'objet de ce guide n'est pas la sécurité de l'information en tant que telle, appliquer les mesures proposées maximise la sécurité du système d'information, berceau des données de votre entité.

La sécurité n'est plus une option. À ce titre, les enjeux de sécurité numérique doivent se rapprocher des préoccupations économiques, stratégiques ou encore d'image qui sont celles des décideurs. En contextualisant le besoin, en rappelant l'objectif poursuivi et en y répondant par la mesure concrète correspondante, ce guide d'hygiène informatique est une feuille de route qui épouse les intérêts de toute entité consciente de la valeur de ses données.

SOMMAIRE

Le présent document comporte 42 règles de sécurité simples. Chacune d'entre elles est importante et vous pouvez tout à fait les considérer indépendamment les unes des autres pour améliorer votre niveau de sécurité sur quelques points particuliers.

Cependant, nous vous conseillons d'utiliser ce guide comme base pour définir un plan d'actions :

1. Commencez par établir un état des lieux pour chacune des règles grâce à l'outil de suivi qui se trouve en annexe de ce document. Pour chaque règle, déterminez si votre organisme atteint le niveau standard et, le cas échéant, le niveau renforcé.
2. Si vous ne pouvez pas faire cet état des lieux par manque de connaissance de votre système d'information, n'hésitez pas à solliciter l'aide d'un spécialiste pour procéder à un diagnostic et assurer un niveau de sécurité élémentaire. (À lire : ANSSI-CGPME, *Guide des bonnes pratiques de l'informatique*, mars 2015).
3. À partir du constat établi à cette première étape, visez en priorité les règles pour lesquelles vous n'avez pas encore atteint le niveau « standard », pour définir un premier plan d'actions. Si les mesures de ce guide doivent être appliquées dans le cadre d'un référentiel publié par l'ANSSI et sauf mention explicite, il s'agit des mesures de niveau « standard ».
4. Lorsque vous avez atteint partout le niveau « standard », vous pouvez définir un nouveau plan d'actions en visant le niveau « renforcé » pour les règles concernées.

I

SENSIBILISER ET FORMER

1 Former les équipes opérationnelles à la sécurité des systèmes d'information

/ STANDARD

Les équipes opérationnelles (administrateurs réseau, sécurité et système, chefs de projet, développeurs, RSSI) ont des accès privilégiés au système d'information. Elles peuvent, par inadvertance ou par méconnaissance des conséquences de certaines pratiques, réaliser des opérations génératrices de vulnérabilités.

Citons par exemple l'affectation de comptes disposant de trop nombreux privilèges par rapport à la tâche à réaliser, l'utilisation de comptes personnels pour exécuter des services ou tâches périodiques, ou encore le choix de mots de passe peu robustes donnant accès à des comptes privilégiés.

Les équipes opérationnelles, pour être à l'état de l'art de la sécurité des systèmes d'information, doivent donc suivre - à leur prise de poste puis à intervalles réguliers - des formations sur :

- la législation en vigueur ;
- les principaux risques et menaces ;
- le maintien en condition de sécurité ;
- l'authentification et le contrôle d'accès ;
- le paramétrage fin et le durcissement des systèmes ;
- le cloisonnement réseau ;
- et la journalisation.

Cette liste doit être précisée selon le métier des collaborateurs en considérant des aspects tels que l'intégration de la sécurité pour les chefs de projet, le développement sécurisé pour les développeurs, les référentiels de sécurité pour les RSSI, etc.
Il est par ailleurs nécessaire de faire mention de clauses spécifiques dans les contrats de prestation pour garantir une formation régulière à la sécurité des systèmes d'information du personnel externe et notamment les infogérants.

2 Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique

/ STANDARD

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation et de formation.

Ces dernières doivent être régulières, adaptées aux utilisateurs ciblés, peuvent prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.) et aborder au minimum les sujets suivants :

- les objectifs et enjeux que rencontre l'entité en matière de sécurité des systèmes d'information ;
- les informations considérées comme sensibles ;
- les réglementations et obligations légales ;
- les règles et consignes de sécurité régissant l'activité quotidienne : respect de la politique de sécurité, non-connexion d'équipements personnels au réseau de l'entité, non-divulgation de mots de passe à un tiers, non-réutilisation de mots de passe professionnels dans la sphère privée et inversement, signalement d'événements suspects, etc. ;
- les moyens disponibles et participant à la sécurité du système : verrouillage systématique de la session lorsque l'utilisateur quitte son poste, outil de protection des mots de passe, etc.

/ RENFORCÉ

Pour renforcer ces mesures, l'élaboration et la signature d'une charte des moyens informatiques précisant les règles et consignes que doivent respecter les utilisateurs peut être envisagée.

3 Maîtriser les risques de l'infogérance

/ STANDARD

Lorsqu'une entité souhaite externaliser son système d'information ou ses données, elle doit en amont évaluer les risques spécifiques à l'infogérance (maîtrise du système d'information, actions à distance, hébergement mutualisé, etc.) afin de prendre en compte, dès la rédaction des exigences applicables au futur prestataire, les besoins et mesures de sécurité adaptés.
Les risques SSI inhérents à ce type de démarche peuvent être liés au contexte de l'opération d'externalisation mais aussi à des spécifications contractuelles déficientes ou incomplètes.

En faveur du bon déroulement des opérations, il s'agit donc :

- d'étudier attentivement les conditions des offres, la possibilité de les adapter à des besoins spécifiques et les limites de responsabilité du prestataire ;
- d'imposer une liste d'exigences précises au prestataire : réversibilité du contrat, réalisation d'audits, sauvegarde et restitution des données dans un format ouvert normalisé, maintien à niveau de la sécurité dans le temps, etc.

Pour formaliser ces engagements, le prestataire fournira au commanditaire un plan d'assurance sécurité (PAS) prévu par l'appel d'offre. Il s'agit d'un document contractuel décrivant l'ensemble des dispositions spécifiques que les candidats s'engagent à mettre en œuvre pour garantir le respect des exigences de sécurité spécifiées par l'entité.

Le recours à des solutions ou outils non maîtrisés (par exemple hébergés dans le nuage) n'est pas ici considéré comme étant du ressort de l'infogérance et par ailleurs déconseillé en cas de traitement d'informations sensibles.

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance*, guide, décembre 2010

II

CONNAÎTRE LE SYSTÈME D'INFORMATION

4 Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau

/STANDARD

Chaque entité possède des données sensibles. Ces dernières peuvent porter sur son activité propre (propriété intellectuelle, savoir-faire, etc.) ou sur ses clients, administrés ou usagers (données personnelles, contrats, etc.). Afin de pouvoir les protéger efficacement, il est indispensable de les identifier.

À partir de cette liste de données sensibles, il sera possible de déterminer sur quels composants du système d'information elles se localisent (bases de données, partages de fichiers, postes de travail, etc.). Ces composants correspondent aux serveurs et postes critiques pour l'entité. À ce titre, ils devront faire l'objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc.

Il s'agit donc de créer et de maintenir à jour un schéma simplifié du réseau (ou cartographie) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma doit également permettre de localiser les serveurs détenteurs d'informations sensibles de l'entité.

5 Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour

/STANDARD

Les comptes bénéficiant de droits spécifiques sont des cibles privilégiées par les attaquants qui souhaitent obtenir un accès le plus large possible au système d'information. Ils doivent donc faire l'objet d'une attention toute particulière. Il s'agit pour cela d'effectuer un inventaire de ces comptes, de le mettre à jour régulièrement et d'y renseigner les informations suivantes :

- les utilisateurs ayant un compte administrateur ou des droits supérieurs à ceux d'un utilisateur standard sur le système d'information ;
- les utilisateurs disposant de suffisamment de droits pour accéder aux répertoires de travail des responsables ou de l'ensemble des utilisateurs ;
- les utilisateurs utilisant un poste non administré par le service informatique et qui ne fait pas l'objet de mesures de sécurité édictées par la politique de sécurité générale de l'entité.

Il est fortement recommandé de procéder à une revue périodique de ces comptes afin de s'assurer que les accès aux éléments sensibles (notamment les répertoires de travail et la messagerie électronique des responsables) soient maitrisés. Ces revues permettront également de supprimer les accès devenus obsolètes suite au départ d'un utilisateur par exemple.

Enfin, il est souhaitable de définir et d'utiliser une nomenclature simple et claire pour identifier les comptes de services et les comptes d'administration. Cela facilitera notamment leur revue et la détection d'intrusion.

6 Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs

/STANDARD

Les effectifs d'une entité, qu'elle soit publique ou privée, évoluent sans cesse : arrivées, départs, mobilité interne. Il est par conséquent nécessaire que les droits et les accès au système d'information soient mis à jour en fonction de ces évolutions. Il est notamment essentiel que l'ensemble des droits affectés à une personne soient révoqués lors de son départ ou en cas de changement de fonction. Les procédures d'arrivée et de départ doivent donc être définies, en lien avec la fonction ressources humaines. Elles doivent au minimum prendre en compte :

- la création et la suppression des comptes informatiques et boîtes aux lettres associées ;
- les droits et accès à attribuer et retirer à une personne dont la fonction change ;
- la gestion des accès physiques aux locaux (attribution, restitution des badges et des clés, etc.) ;
- l'affectation des équipements mobiles (ordinateur portable, clé USB, disque dur, ordiphone, etc.) ;
- la gestion des documents et informations sensibles (transfert de mots de passe, changement des mots de passe ou des codes sur les systèmes existants).

/RENFORCÉ

Les procédures doivent être formalisées et mises à jour en fonction du contexte.

7 Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés

/STANDARD

Pour garantir la sécurité de son système d'information, l'entité doit maîtriser les équipements qui s'y connectent, chacun constituant un point d'entrée potentiellement vulnérable. Les équipements personnels (ordinateurs portables, tablettes, ordiphones, etc.) sont, par définition, difficilement maîtrisables dans la mesure où ce sont les utilisateurs qui décident de leur niveau de sécurité. De la même manière, la sécurité des équipements dont sont dotés les visiteurs échappe à tout contrôle de l'entité.

Seule la connexion de terminaux maîtrisés par l'entité doit être autorisée sur ses différents réseaux d'accès, qu'ils soient filaire ou sans fil. Cette recommandation, avant tout d'ordre organisationnel, est souvent perçue comme inacceptable ou rétrograde. Cependant, y déroger fragilise le réseau de l'entité et sert ainsi les intérêts d'un potentiel attaquant.

La sensibilisation des utilisateurs doit donc s'accompagner de solutions pragmatiques répondant à leurs besoins. Citons par exemple la mise à disposition d'un réseau Wi-Fi avec SSID dédié pour les terminaux personnels ou visiteurs.

/RENFORCÉ

Ces aménagements peuvent être complétés par des mesures techniques telles que l'authentification des postes sur le réseau (par exemple à l'aide du standard 802.1X ou d'un équivalent).

III

AUTHENTIFIER ET CONTRÔLER LES ACCÈS

8 Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur

/STANDARD

Afin de faciliter l'attribution d'une action sur le système d'information en cas d'incident ou d'identifier d'éventuels comptes compromis, les comptes d'accès doivent être nominatifs.

L'utilisation de comptes génériques (ex : *admin*, *user*) doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques.

Bien entendu, cette règle n'interdit pas le maintien de comptes de service, rattachés à un processus informatique (ex : *apache*, *mysqld*).

Dans tous les cas, les comptes génériques et de service doivent être gérés selon une politique au moins aussi stricte que celle des comptes nominatifs. Par ailleurs, un compte d'administration nominatif, distinct du compte utilisateur, doit être attribué à chaque administrateur. Les identifiants et secrets d'authentification doivent être différents (ex : *pmartin* comme identifiant utilisateur, *adm-pmartin* comme identifiant administrateur). Ce compte d'administration, disposant de plus de privilèges, doit être dédié exclusivement aux actions d'administration. De plus, il doit être utilisé sur des environnements dédiés à l'administration afin de ne pas laisser de traces de connexion ni de condensat de mot de passe sur un environnement plus exposé.

/RENFORCÉ

Dès que possible la journalisation liée aux comptes (ex : relevé des connexions réussies/échouées) doit être activée.

9 Attribuer les bons droits sur les ressources sensibles du système d'information

/STANDARD

Certaines des ressources du système peuvent constituer une source d'information précieuse aux yeux d'un attaquant (répertoires contenant des données sensibles, bases de données, boîtes aux lettres électroniques, etc.). Il est donc primordial d'établir une liste précise de ces ressources et pour chacune d'entre elles :

- de définir quelle population peut y avoir accès ;
- de contrôler strictement son accès, en s'assurant que les utilisateurs sont authentifiés et font partie de la population ciblée ;
- d'éviter sa dispersion et sa duplication à des endroits non maîtrisés ou soumis à un contrôle d'accès moins strict.

Par exemple, les répertoires des administrateurs regroupant de nombreuses informations sensibles doivent faire l'objet d'un contrôle d'accès précis. Il en va de même pour les informations sensibles présentes sur des partages réseau : exports de fichiers de configuration, documentation technique du système d'information, bases de données métier, etc. Une revue régulière des droits d'accès doit par ailleurs être réalisée afin d'identifier les accès non autorisés.

10 Définir et vérifier des règles de choix et de dimensionnement des mots de passe

/STANDARD

L'ANSSI énonce un ensemble de règles et de bonnes pratiques en matière de choix et de dimensionnement des mots de passe. Parmi les plus critiques de ces règles figure la sensibilisation des utilisateurs aux risques liés au choix d'un mot de passe qui serait trop facile à deviner, ou encore la réutilisation de mots de passe d'une application à l'autre et plus particulièrement entre messageries personnelles et professionnelles.

Pour encadrer et vérifier l'application de ces règles de choix et de dimensionnement, l'entité pourra recourir à différentes mesures parmi lesquelles :

> le blocage des comptes à l'issue de plusieurs échecs de connexion ;
> la désactivation des options de connexion anonyme ;
> l'utilisation d'un outil d'audit de la robustesse des mots de passe.

En amont de telles procédures, un effort de communication visant à expliquer le sens de ces règles et éveiller les consciences sur leur importance est fondamental.

ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012

11 Protéger les mots de passe stockés sur les systèmes

/STANDARD

La complexité, la diversité ou encore l'utilisation peu fréquente de certains mots de passe, peuvent encourager leur stockage sur un support physique (mémo, post-it) ou numérique (fichiers de mots de passe, envoi par mail à soi-même, recours aux boutons « Se souvenir du mot de passe ») afin de pallier tout oubli ou perte.

Or, les mots de passe sont une cible privilégiée par les attaquants désireux d'accéder au système, que cela fasse suite à un vol ou à un éventuel partage du support de stockage. C'est pourquoi ils doivent impérativement être protégés au moyen de solutions sécurisées au premier rang desquelles figurent l'utilisation d'un coffre-fort numérique et le recours à des mécanismes de chiffrement.

Bien entendu, le choix d'un mot de passe pour ce coffre-fort numérique doit respecter les règles énoncées précédemment et être mémorisé par l'utilisateur, qui n'a plus que celui-ci à retenir.

12 Changer les éléments d'authentification par défaut sur les équipements et services

/STANDARD

Il est impératif de partir du principe que les configurations par défaut des systèmes d'information sont systématiquement connues des attaquants, quand bien même celles-ci ne le sont pas du grand public. Ces configurations se révèlent (trop) souvent triviales (mot de passe identique à l'identifiant, mal dimensionné ou commun à l'ensemble des équipements et services par exemple) et sont, la plupart du temps, faciles à obtenir pour des attaquants capables de se faire passer pour un utilisateur légitime.

Les éléments d'authentification par défaut des composants du système doivent donc être modifiés dès leur installation et, s'agissant de mots de passe, être conformes aux recommandations précédentes en matière de choix, de dimensionnement et de stockage.

Si le changement d'un identifiant par défaut se révèle impossible pour cause, par exemple, de mot de passe ou certificat « en dur » dans un équipement, ce problème critique doit être signalé au distributeur du produit afin que cette vulnérabilité soit corrigée au plus vite.

/RENFORCÉ

Afin de limiter les conséquences d'une compromission, il est par ailleurs essentiel, après changement des éléments d'authentification par défaut, de procéder à leur renouvellement régulier.

13 Privilégier lorsque c'est possible une authentification forte

/STANDARD

Il est vivement recommandé de mettre en œuvre une authentification forte nécessitant l'utilisation de deux facteurs d'authentification différents parmi les suivants :

> quelque chose que je sais (mot de passe, tracé de déverrouillage, signature) ;
> quelque chose que je possède (carte à puce, jeton USB, carte magnétique, RFID, un téléphone pour recevoir un code SMS) ;
> quelque chose que je suis (une empreinte biométrique).

/RENFORCÉ

Les cartes à puces doivent être privilégiées ou, à défaut, les mécanismes de mots de passe à usage unique (ou *One Time Password*) avec jeton physique. Les opérations cryptographiques mises en place dans ces deux facteurs offrent généralement de bonnes garanties de sécurité.

Les cartes à puce peuvent être plus complexes à mettre en place car nécessitant une infrastructure de gestion des clés adaptée. Elles présentent cependant l'avantage d'être réutilisables à plusieurs fins : chiffrement, authentification de messagerie, authentification sur le poste de travail, etc.

IV

SÉCURISER LES POSTES

14 Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique

/STANDARD

L'utilisateur plus ou moins au fait des bonnes pratiques de sécurité informatique est, dans de très nombreux cas, la première porte d'entrée des attaquants vers le système. Il est donc fondamental de mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique de l'entité (postes utilisateurs, serveurs, imprimantes, téléphones, périphériques USB, etc.) en implémentant les mesures suivantes :

- limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires ;
- doter les postes utilisateurs d'un pare-feu local et d'un anti-virus (ceux-ci sont parfois inclus dans le système d'exploitation) ;
- chiffrer les partitions où sont stockées les données des utilisateurs ;
- désactiver les exécutions automatiques (autorun).

En cas de dérogation nécessaire aux règles de sécurité globales applicables aux postes, ceux-ci doivent être isolés du système (s'il est impossible de mettre à jour certaines applications pour des raisons de compatibilité par exemple).

/RENFORCÉ

Les données vitales au bon fonctionnement de l'entité que détiennent les postes utilisateurs et les serveurs doivent faire l'objet de sauvegardes régulières et stockées sur des équipements déconnectés, et leur restauration doit être vérifiée de manière périodique. En effet, de plus en plus de petites structures font l'objet d'attaques rendant ces données indisponibles (par exemple pour exiger en contrepartie de leur restitution le versement d'une somme conséquente (rançongiciel)).

15 Se protéger des menaces relatives à l'utilisation de supports amovibles

/STANDARD

Les supports amovibles peuvent être utilisés afin de propager des virus, voler des informations sensibles et stratégiques ou encore compromettre le réseau de l'entité. De tels agissements peuvent avoir des conséquences désastreuses pour l'activité de la structure ciblée.

S'il n'est pas question d'interdire totalement l'usage de supports amovibles au sein de l'entité, il est néanmoins nécessaire de traiter ces risques en identifiant des mesures adéquates et en sensibilisant les utilisateurs aux risques que ces supports peuvent véhiculer.

Il convient notamment de proscrire le branchement de clés USB inconnues (ramassées dans un lieu public par exemple) et de limiter au maximum celui de clés non maîtrisées (dont on connait la provenance mais pas l'intégrité) sur le système d'information à moins, dans ce dernier cas, de faire inspecter leur contenu par l'antivirus du poste de travail.

/RENFORCÉ

Sur les postes utilisateur, il est recommandé d'utiliser des solutions permettant d'interdire l'exécution de programmes sur les périphériques amovibles (par exemple Applocker sous Windows ou des options de montage *noexec* sous Unix).

Lors de la fin de vie des supports amovibles, il sera nécessaire d'implémenter et de respecter une procédure de mise au rebut stricte pouvant aller jusqu'à leur destruction sécurisée afin de limiter la fuite d'informations sensibles.

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*, note technique, décembre 2013

ANSSI, *Recommandations de configuration d'un système GNU/Linux*, note technique, janvier 2016

16 Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité

/STANDARD

La sécurité du système d'information repose sur la sécurité du maillon le plus faible. Il est donc nécessaire d'homogénéiser la gestion des politiques de sécurité s'appliquant à l'ensemble du parc informatique de l'entité.

L'application de ces politiques (gestion des mots de passe, restrictions de connexions sur certains postes sensibles, configuration des navigateurs Web, etc.) doit être simple et rapide pour les administrateurs, en vue notamment de faciliter la mise en œuvre de contre-mesures en cas de crise informatique.

Pour cela, l'entité pourra se doter d'un outil de gestion centralisée (par exemple Active Directory en environnement Microsoft) auquel il s'agit d'inclure le plus grand nombre d'équipements informatiques possible. Les postes de travail et les serveurs sont concernés par cette mesure qui nécessite éventuellement en amont un travail d'harmonisation des choix de matériels et de systèmes d'exploitation.

Ainsi, des politiques de durcissement du système d'exploitation ou d'applications pourront facilement s'appliquer depuis un point central tout en favorisant la réactivité attendue en cas de besoin de reconfiguration.

ANSSI, *Recommandations de sécurité relatives à Active Directory*, note technique, septembre 2014

17 Activer et configurer le pare-feu local des postes de travail

/STANDARD

Après avoir réussi à prendre le contrôle d'un poste de travail (à cause, par exemple, d'une vulnérabilité présente dans le navigateur Internet), un attaquant cherchera souvent à étendre son intrusion aux autres postes de travail pour, *in fine*, accéder aux documents des utilisateurs.

Afin de rendre plus difficile ce déplacement latéral de l'attaquant, il est nécessaire d'activer le pare-feu local des postes de travail au moyen de logiciels intégrés (pare-feu local Windows) ou spécialisés.

Les flux de poste à poste sont en effet très rares dans un réseau bureautique classique : les fichiers sont stockés dans des serveurs de fichiers, les applications accessibles sur des serveurs métier, etc.

/RENFORCÉ

Le filtrage le plus simple consiste à bloquer l'accès aux ports d'administration par défaut des postes de travail (ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix), excepté depuis les ressources explicitement identifiées (postes d'administration et d'assistance utilisateur, éventuels serveurs de gestion requérant l'accès à des partages réseau sur les postes, etc.).

Une analyse des flux entrants utiles (administration, logiciels d'infrastructure, applications particulières, etc.) doit être menée pour définir la liste des autorisations à configurer. Il est préférable de bloquer l'ensemble des flux par défaut et de n'autoriser que les services nécessaires depuis les équipements correspondants (« liste blanche »).

Le pare-feu doit également être configuré pour journaliser les flux bloqués, et ainsi identifier les erreurs de configuration d'applications ou les tentatives d'intrusion.

18 Chiffrer les données sensibles transmises par voie Internet

/STANDARD

Internet est un réseau sur lequel il est quasi impossible d'obtenir des garanties sur le trajet que vont emprunter les données que l'on y envoie. Il est donc tout à fait possible qu'un attaquant se trouve sur le trajet de données transitant entre deux correspondants.

Toutes les données envoyées par courriel ou transmises au moyen d'outils d'hébergement en ligne (Cloud) sont par conséquent vulnérables. Il s'agit donc de procéder à leur chiffrement systématique avant de les adresser à un correspondant ou de les héberger.

La transmission du secret (mot de passe, clé, etc.) permettant alors de déchiffrer les données, si elle est nécessaire, doit être effectuée via un canal de confiance ou, à défaut, un canal distinct du canal de transmission des données. Ainsi, si les données chiffrées sont transmises par courriel, une remise en main propre du mot de passe ou, à défaut, par téléphone doit être privilégiée.

Catalogue des produits et prestataires de service qualifiés

V

SÉCURISER LE RÉSEAU

19 Segmenter le réseau et mettre en place un cloisonnement entre ces zones

/STANDARD

Lorsque le réseau est « à plat », sans aucun mécanisme de cloisonnement, chaque machine du réseau peut accéder à n'importe quelle autre machine. La compromission de l'une d'elles met alors en péril l'ensemble des machines connectées. Un attaquant peut ainsi compromettre un poste utilisateur et ensuite « rebondir » jusqu'à des serveurs critiques.

Il est donc important, dès la conception de l'architecture réseau, de raisonner par segmentation en zones composées de systèmes ayant des besoins de sécurité homogènes. On pourra par exemple regrouper distinctement des serveurs d'infrastructure, des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc.

Une zone se caractérise alors par des VLAN et des sous-réseaux IP dédiés voire par des infrastructures dédiées selon sa criticité. Ainsi, des mesures de cloisonnement telles qu'un filtrage IP à l'aide d'un pare-feu peuvent être mises en place entre les différentes zones. On veillera en particulier à cloisonner autant que possible les équipements et flux associés aux tâches d'administration.

Pour les réseaux dont le cloisonnement a posteriori ne serait pas aisé, il est recommandé d'intégrer cette démarche dans toute nouvelle extension du réseau ou à l'occasion d'un renouvellement d'équipements.

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

20 S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages

/STANDARD

L'usage du Wi-Fi en milieu professionnel est aujourd'hui démocratisé mais présente toujours des risques de sécurité bien spécifiques : faibles garanties en matière de disponibilité, pas de maîtrise de la zone de couverture pouvant mener à une attaque hors du périmètre géographique de l'entité, configuration par défaut des points d'accès peu sécurisée, etc.

La segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion par voie radio à un périmètre déterminé du système d'information. Les flux en provenance des postes connectés au réseau d'accès Wi-Fi doivent donc être filtrés et restreints aux seuls flux nécessaires.

De plus, il est important d'avoir recours prioritairement à un chiffrement robuste (mode WPA2, algorithme AES CCMP) et à une authentification centralisée, si possible par certificats clients des machines.

La protection du réseau Wi-Fi par un mot de passe unique et partagé est déconseillée. À défaut, il doit être complexe et son renouvellement prévu mais il ne doit en aucun cas être diffusé à des tiers non autorisés.

Les points d'accès doivent par ailleurs être administrés de manière sécurisée (ex : interface dédiée, modification du mot de passe administrateur par défaut).

Enfin, toute connexion Wi-Fi de terminaux personnels ou visiteurs (ordinateurs portables, ordiphones) doit être séparée des connexions Wi-Fi des terminaux de l'entité (ex : SSID et VLAN distincts, accès Internet dédié).

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi*, note technique, septembre 2013

21 Utiliser des protocoles réseaux sécurisés dès qu'ils existent

/STANDARD

Si aujourd'hui la sécurité n'est plus optionnelle, cela n'a pas toujours été le cas. C'est pourquoi de nombreux protocoles réseaux ont dû évoluer pour intégrer cette composante et répondre aux besoins de confidentialité et d'intégrité qu'impose l'échange de données. Les protocoles réseaux sécurisés doivent être utilisés dès que possible, que ce soit sur des réseaux publics (Internet par exemple) ou sur le réseau interne de l'entité.

Bien qu'il soit difficile d'en dresser une liste exhaustive, les protocoles les plus courants reposent sur l'utilisation de TLS et sont souvent identifiables par l'ajout de la lettre « s » (pour *secure* en anglais) à l'acronyme du protocole. Citons par exemple HTTPS pour la navigation Web ou IMAPS, SMTPS ou POP3S pour la messagerie.

D'autres protocoles ont été conçus de manière sécurisée dès la conception pour se substituer à d'anciens protocoles non sécurisés. Citons par exemple SSH (*Secure SHell*) venu remplacer les protocoles de communication historiques TELNET et RLOGIN.

ANSSI, *Recommandations pour un usage sécurisé d'[OPEN] SSH*, note technique, août 2016

22 Mettre en place une passerelle d'accès sécurisé à Internet

/STANDARD

L'accès à Internet, devenu indispensable, présente des risques importants : sites Web hébergeant du code malveillant, téléchargement de fichiers « toxiques » et, par conséquent, possible prise de contrôle du terminal, fuite de données sensibles, etc. Pour sécuriser cet usage, il est donc indispensable que les terminaux utilisateurs n'aient pas d'accès réseau direct à Internet.

C'est pourquoi il est recommandé de mettre en œuvre une passerelle sécurisée d'accès à Internet comprenant au minimum un pare-feu au plus près de l'accès Internet pour filtrer les connexions et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité. Celui-ci assure notamment l'authentification des utilisateurs et la journalisation des requêtes.

/RENFORCÉ

Des mécanismes complémentaires sur le serveur mandataire pourront être activés selon les besoins de l'entité : analyse antivirus du contenu, filtrage par catégories d'URLs, etc. Le maintien en condition de sécurité des équipements de la passerelle est essentiel, il fera donc l'objet de procédures à respecter. Suivant le nombre de collaborateurs et le besoin de disponibilité, ces équipements pourront être redondés.

Par ailleurs, pour les terminaux utilisateurs, les résolutions DNS en direct de noms de domaines publics seront par défaut désactivées, celles-ci étant déléguées au serveur mandataire.

Enfin, il est fortement recommandé que les postes nomades établissent au préalable une connexion sécurisée au système d'information de l'entité pour naviguer de manière sécurisée sur le Web à travers la passerelle.

23 Cloisonner les services visibles depuis Internet du reste du système d'information

/STANDARD

Une entité peut choisir d'héberger en interne des services visibles sur Internet (site web, serveur de messagerie, etc.). Au regard de l'évolution et du perfectionnement des cyberattaques sur Internet, il est essentiel de garantir un haut niveau de protection de ce service avec des administrateurs compétents, formés de manière continue (à l'état de l'art des technologies en la matière) et disponibles. Dans le cas contraire, le recours à un hébergement externalisé auprès de professionnels est à privilégier.

De plus, les infrastructures d'hébergement Internet doivent être physiquement cloisonnées de toutes les infrastructures du système d'information qui n'ont pas vocation à être visibles depuis Internet.

Enfin, il convient de mettre en place une infrastructure d'interconnexion de ces services avec Internet permettant de filtrer les flux liés à ces services de manière distincte des autres flux de l'entité. Il s'agit également d'imposer le passage des flux entrants par un serveur mandataire inverse (*reverse proxy*) embarquant différents mécanismes de sécurité.

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée*, note technique, décembre 2011

ANSSI, *Maîtriser les risques de l'infogérance*, guide, décembre 2010

24 Protéger sa messagerie professionnelle

/STANDARD

La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant.

Les utilisateurs doivent être particulièrement sensibilisés à ce sujet : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) est nécessaire.

Pour se prémunir d'escroqueries (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue une fuite irrémédiable d'informations de l'entité. Si nécessaire des moyens maîtrisés et sécurisés pour l'accès distant à la messagerie professionnelle doivent être proposés.

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

- de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ;
- de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes aux lettres.

/RENFORCÉ

Il est souhaitable de ne pas exposer directement les serveurs de boîte aux lettres sur Internet. Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

Alors que le spam - malveillant ou non - constitue la majorité des courriels échangés sur Internet, le déploiement d'un service anti-spam doit permettre d'éliminer cette source de risques.

Enfin, l'administrateur de messagerie s'assurera de la mise en place des mécanismes de vérification d'authenticité et de la bonne configuration des enregistrements DNS publics liés à son infrastructure de messagerie (MX, SPF, DKIM, DMARC).

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, guide, février 2015

25 Sécuriser les interconnexions réseau dédiées avec les partenaires

/STANDARD

Pour des besoins opérationnels, une entité peut être amenée à établir une interconnexion réseau dédiée avec un fournisseur ou un client (ex : infogérance, échange de données informatisées, flux monétiques, etc.).

Cette interconnexion peut se faire au travers d'un lien sur le réseau privé de l'entité ou directement sur Internet. Dans le second cas, il convient d'établir un tunnel site à site, de préférence IPsec, en respectant les préconisations de l'ANSSI.

Le partenaire étant considéré par défaut comme non sûr, il est indispensable d'effectuer un filtrage IP à l'aide d'un pare-feu au plus près de l'entrée des flux sur le réseau de l'entité. La matrice des flux (entrants et sortants) devra être réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements devra y être conforme.

/RENFORCÉ

Pour des entités ayant des besoins de sécurité plus exigeants, il conviendra de s'assurer que l'équipement de filtrage IP pour les connexions partenaires est dédié à cet usage. L'ajout d'un équipement de détection d'intrusions peut également constituer une bonne pratique.

Par ailleurs la connaissance d'un point de contact à jour chez le partenaire est nécessaire pour pouvoir réagir en cas d'incident de sécurité.

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013

26 Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques

/STANDARD

Les mécanismes de sécurité physique doivent faire partie intégrante de la sécurité des systèmes d'information et être à l'état de l'art afin de s'assurer qu'ils ne puissent pas être contournés aisément par un attaquant. Il convient donc d'identifier les mesures de sécurité physique adéquates et de sensibiliser continuellement les utilisateurs aux risques engendrés par le contournement des règles.

Les accès aux salles serveurs et aux locaux techniques doivent être contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont à proscrire, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires. Une revue des droits d'accès doit être réalisée régulièrement afin d'identifier les accès non autorisés.

Lors du départ d'un collaborateur ou d'un changement de prestataire, il est nécessaire de procéder au retrait des droits d'accès ou au changement des codes d'accès.

Enfin, les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) doivent être restreintes ou désactivées afin d'empêcher un attaquant de gagner facilement l'accès au réseau de l'entreprise.

VI

SÉCURISER L'ADMINISTRATION

27 Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information

/STANDARD

Un poste de travail ou un serveur utilisé pour les actions d'administration ne doit en aucun cas avoir accès à Internet, en raison des risques que la navigation Web (à travers des sites contenant du code malveillant) et la messagerie (au travers de pièces jointes potentiellement vérolées) font peser sur son intégrité.

Pour les autres usages des administrateurs nécessitant Internet (consultation de documentation en ligne, de leur messagerie, etc.), il est recommandé de mettre à leur disposition un poste de travail distinct. À défaut, l'accès à une infrastructure virtualisée distante pour la bureautique depuis un poste d'administration est envisageable. La réciproque consistant à fournir un accès distant à une infrastructure d'administration depuis un poste bureautique est déconseillée car elle peut mener à une élévation de privilèges en cas de récupération des authentifiants d'administration.

/RENFORCÉ

Concernant les mises à jour logicielles des équipements administrés, elles doivent être récupérées depuis une source sûre (le site de l'éditeur par exemple), contrôlées puis transférées sur le poste ou le serveur utilisé pour l'administration et non connecté à Internet. Ce transfert peut être réalisé sur un support amovible dédié.

Pour des entités voulant automatiser certaines tâches, la mise en place d'une zone d'échanges est conseillée.

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015

28 Utiliser un réseau dédié et cloisonné pour l'administration du système d'information

/STANDARD

Un réseau d'administration interconnecte, entre autres, les postes ou serveurs d'administration et les interfaces d'administration des équipements. Dans la logique de segmentation du réseau global de l'entité, il est indispensable de cloisonner spécifiquement le réseau d'administration, notamment vis-à-vis du réseau bureautique des utilisateurs, pour se prémunir de toute compromission par rebond depuis un poste utilisateur vers une ressource d'administration.

Selon les besoins de sécurité de l'entité, il est recommandé :

- de privilégier en premier lieu un cloisonnement physique des réseaux dès que cela est possible, cette solution pouvant représenter des coûts et un temps de déploiement importants ; /RENFORCÉ
- à défaut, de mettre en œuvre un cloisonnement logique cryptographique reposant sur la mise en place de tunnels IPsec. Ceci permet d'assurer l'intégrité et la confidentialité des informations véhiculées sur le réseau d'administration vis-à-vis du réseau bureautique des utilisateurs ; /STANDARD
- au minimum, de mettre en œuvre un cloisonnement logique par VLAN. /STANDARD

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015

29 Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail

/STANDARD

De nombreux utilisateurs, y compris au sommet des hiérarchies, sont tentés de demander à leur service informatique de pouvoir disposer, par analogie avec leur usage personnel, de privilèges plus importants sur leurs postes de travail : installation de logiciels, configuration du système, etc. Par défaut, il est recommandé qu'un utilisateur du SI, quelle que soit sa position hiérarchique et ses attributions, ne dispose pas de privilèges d'administration sur son poste de travail. Cette mesure, apparemment contraignante, vise à limiter les conséquences de l'exécution malencontreuse d'un code malveillant. La mise à disposition d'un magasin étoffé d'applications validées par l'entité du point de vue de la sécurité permettra de répondre à la majorité des besoins.

Par conséquent, seuls les administrateurs chargés de l'administration des postes doivent disposer de ces droits lors de leurs interventions.

Si une délégation de privilèges sur un poste de travail est réellement nécessaire pour répondre à un besoin ponctuel de l'utilisateur, celle-ci doit être tracée, limitée dans le temps et retirée à échéance.

VII

GÉRER LE NOMADISME

30 Prendre des mesures de sécurisation physique des terminaux nomades

/STANDARD

Les terminaux nomades (ordinateurs portables, tablettes, ordiphones) sont, par nature, exposés à la perte et au vol. Ils peuvent contenir localement des informations sensibles pour l'entité et constituer un point d'entrée vers de plus amples ressources du système d'information. Au-delà de l'application au minimum des politiques de sécurité de l'entité, des mesures spécifiques de sécurisation de ces équipements sont donc à prévoir.

En tout premier lieu, les utilisateurs doivent être sensibilisés pour augmenter leur niveau de vigilance lors de leurs déplacements et conserver leurs équipements à portée de vue. N'importe quelle entité, même de petite taille, peut être victime d'une attaque informatique. Dès lors, en mobilité, tout équipement devient une cible potentielle voire privilégiée.

Il est recommandé que les terminaux nomades soient aussi banalisés que possible en évitant toute mention explicite de l'entité d'appartenance (par l'apposition d'un autocollant aux couleurs de l'entité par exemple).

Pour éviter toute indiscrétion lors de déplacements, notamment dans les transports ou les lieux d'attente, un filtre de confidentialité doit être positionné sur chaque écran.

/RENFORCÉ

Enfin, afin de rendre inutilisable le poste seul, l'utilisation d'un support externe complémentaire (carte à puce ou jeton USB par exemple) pour conserver des secrets de déchiffrement ou d'authentification peut être envisagée. Dans ce cas il doit être conservé à part.

ANSSI-CDSE, *Passeport de conseils aux voyageurs*, bonnes pratiques, janvier 2010

31 Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable

/STANDARD

Les déplacements fréquents en contexte professionnel et la miniaturisation du matériel informatique conduisent souvent à la perte ou au vol de celui-ci dans l'espace public. Cela peut porter atteinte aux données sensibles de l'entité qui y sont stockées.

Il faut donc ne stocker que des données préalablement chiffrées sur l'ensemble des matériels nomades (ordinateurs portables, ordiphones, clés USB, disques durs externes, etc.) afin de préserver leur confidentialité. Seul un secret (mot de passe, carte à puce, code PIN, etc.) pourra permettre à celui qui le possède d'accéder à ces données.

Une solution de chiffrement de partition, d'archives ou de fichier peut être envisagée selon les besoins. Là encore, il est essentiel de s'assurer de l'unicité et de la robustesse du secret de déchiffrement utilisé.

Dans la mesure du possible, il est conseillé de commencer par un chiffrement complet du disque avant d'envisager le chiffrement d'archives ou de fichiers. En effet, ces derniers répondent à des besoins différents et peuvent potentiellement laisser sur le support de stockage des informations non chiffrées (fichiers de restauration de suite bureautique, par exemple).

Catalogue des produits et prestataires de service qualifiés

32 Sécuriser la connexion réseau des postes utilisés en situation de nomadisme

/STANDARD

En situation de nomadisme, il n'est pas rare qu'un utilisateur ait besoin de se connecter au système d'information de l'entité. Il convient par conséquent de s'assurer du caractère sécurisé de cette connexion réseau à travers Internet. Même si la possibilité d'établir des tunnels VPN SSL/TLS est aujourd'hui courante, il est fortement recommandé d'établir un tunnel VPN IPsec entre le poste nomade et une passerelle VPN IPsec mise à disposition par l'entité.

Pour garantir un niveau de sécurité optimal, ce tunnel VPN IPsec doit être automatiquement établi et ne pas être débrayable par l'utilisateur, c'est-à-dire qu'aucun flux ne doit pouvoir être transmis en dehors de ce tunnel.

Pour les besoins spécifiques d'authentification aux portails captifs, l'entité peut choisir de déroger à la connexion automatique en autorisant une connexion à la demande ou maintenir cette recommandation en encourageant l'utilisateur à utiliser un partage de connexion sur un téléphone mobile de confiance.

/RENFORCÉ

Afin d'éviter toute réutilisation d'authentifiants depuis un poste volé ou perdu (identifiant et mot de passe enregistrés par exemple), il est préférable d'avoir recours à une authentification forte, par exemple avec un mot de passe et un certificat stocké sur un support externe (carte à puce ou jeton USB) ou un mécanisme de mot de passe à usage unique (*One Time Password*).

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015

33 Adopter des politiques de sécurité dédiées aux terminaux mobiles

/STANDARD

Les ordiphones et tablettes font partie de notre quotidien personnel et/ou professionnel. La première des recommandations consiste justement à ne pas mutualiser les usages personnel et professionnel sur un seul et même terminal, par exemple en ne synchronisant pas simultanément comptes professionnel et personnel de messagerie, de réseaux sociaux, d'agendas, etc.

Les terminaux, fournis par l'entité et utilisés en contexte professionnel doivent faire l'objet d'une sécurisation à part entière, dès lors qu'ils se connectent au système d'information de l'entité ou qu'ils contiennent des informations professionnelles potentiellement sensibles (mails, fichiers partagés, contacts, etc.). Dès lors, l'utilisation d'une solution de gestion centralisée des équipements mobiles est à privilégier. Il sera notamment souhaitable de configurer de manière homogène les politiques de sécurité inhérentes : moyen de déverrouillage du terminal, limitation de l'usage du magasin d'applications à des applications validées du point de vue de la sécurité, etc.

Dans le cas contraire, une configuration préalable avant remise de l'équipement et une séance de sensibilisation des utilisateurs est souhaitable.

/RENFORCÉ

Entre autres usages potentiellement risqués, celui d'un assistant vocal intégré augmente sensiblement la surface d'attaque du terminal et des cas d'attaque ont été démontrés. Pour ces raisons, il est donc déconseillé.

ANSSI, *Recommandations de sécurité relatives aux ordiphones*, note technique, juillet 2015

VIII

MAINTENIR LE SYSTÈME D'INFORMATION À JOUR

34 Définir une politique de mise à jour des composants du système d'information

/STANDARD

De nouvelles failles sont régulièrement découvertes au cœur des systèmes et logiciels. Ces dernières sont autant de portes d'accès qu'un attaquant peut exploiter pour réussir son intrusion dans le système d'information. Il est donc primordial de s'informer de l'apparition de nouvelles vulnérabilités (CERT-FR) et d'appliquer les correctifs de sécurité sur l'ensemble des composants du système dans le mois qui suit leur publication par l'éditeur. Une politique de mise à jour doit ainsi être définie et déclinée en procédures opérationnelles.

Celles-ci doivent notamment préciser :

- la manière dont l'inventaire des composants du système d'information est réalisé ;
- les sources d'information relatives à la publication des mises à jour ;
- les outils pour déployer les correctifs sur le parc (par exemple WSUS pour les mises à jour des composants Microsoft, des outils gratuits ou payants pour les composants tiers et autres systèmes d'exploitation) ;
- l'éventuelle qualification des correctifs et leur déploiement progressif sur le parc.

Les composants obsolètes qui ne sont plus supportés par leurs fabricants doivent être isolés du reste du système. Cette recommandation s'applique aussi bien au niveau réseau par un filtrage strict des flux, qu'au niveau des secrets d'authentification qui doivent être dédiés à ces systèmes.

CERT-FR : au sein du COSSI, le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) assure le rôle de CERT (pour Computer Emergency Response Team) gouvernemental français. À ce titre, il compte parmi ses missions principales une action de veille technologique informant tout un chacun sur l'état de l'art des systèmes et logiciels.

35 Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles

/STANDARD

L'utilisation d'un système ou d'un logiciel obsolète augmente significativement les possibilités d'attaque informatique. Les systèmes deviennent vulnérables dès lors que les correctifs ne sont plus proposés. En effet, des outils malveillants exploitant ces vulnérabilités peuvent se diffuser rapidement sur Internet alors même que l'éditeur ne propose pas de correctif de sécurité.

Pour anticiper ces obsolescences, un certain nombre de précautions existent :

- établir et tenir à jour un inventaire des systèmes et applications du système d'information ;
- choisir des solutions dont le support est assuré pour une durée correspondant à leur utilisation ;
- assurer un suivi des mises à jour et des dates de fin de support des logiciels ;
- maintenir un parc logiciel homogène (la coexistence de versions différentes d'un même produit multiplie les risques et complique le suivi) ;
- limiter les adhérences logicielles, c'est-à-dire les dépendances de fonctionnement d'un logiciel par rapport à un autre, en particulier lorsque le support de ce dernier arrive à son terme ;
- inclure dans les contrats avec les prestataires et fournisseurs des clauses garantissant le suivi des correctifs de sécurité et la gestion des obsolescences ;
- identifier les délais et ressources nécessaires (matérielles, humaines, budgétaires) à la migration de chaque logiciel en fin de vie (tests de non-régression, procédure de sauvegarde, procédure de migration des données, etc.).

IX

SUPERVISER, AUDITER, RÉAGIR

36 Activer et configurer les journaux des composants les plus importants

/STANDARD

Disposer de journaux pertinents est nécessaire afin de pouvoir détecter d'éventuels dysfonctionnements et tentatives d'accès illicites aux composants du système d'information.

La première étape consiste à déterminer quels sont les composants critiques du système d'information. Il peut notamment s'agir des équipements réseau et de sécurité, des serveurs critiques, des postes de travail d'utilisateurs sensibles, etc.

Pour chacun, il convient d'analyser la configuration des éléments journalisés (format, fréquence de rotation des fichiers, taille maximale des fichiers journaux, catégories d'évènements enregistrés, etc.) et de l'adapter en conséquence. Les évènements critiques pour la sécurité doivent être journalisés et gardés pendant au moins un an (ou plus en fonction des obligations légales du secteur d'activités).

Une étude contextuelle du système d'information doit être effectuée et les éléments suivants doivent être journalisés :

- pare-feu : paquets bloqués ;
- systèmes et applications : authentifications et autorisations (échecs et succès), arrêts inopinés ;
- services : erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP), traçabilité des flux applicatifs aux interconnexions (URL sur un relai HTTP, en-têtes des messages sur un relai SMTP, etc.) ;

Afin de pouvoir corréler les évènements entre les différents composants, leur source de synchronisation de temps (grâce au protocole NTP) doit être identique.

/RENFORCÉ

Si toutes les actions précédentes ont été mises en œuvre, une centralisation des journaux sur un dispositif dédié pourra être envisagée. Cela permet de faciliter la recherche automatisée d'événements suspects, d'archiver les journaux sur une longue durée et d'empêcher un attaquant d'effacer d'éventuelles traces de son passage sur les équipements qu'il a compromis.

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013

37 Définir et appliquer une politique de sauvegarde des composants critiques

/STANDARD

Suite à un incident d'exploitation ou en contexte de gestion d'une intrusion, la disponibilité de sauvegardes conservées en lieu sûr est indispensable à la poursuite de l'activité. Il est donc fortement recommandé de formaliser une politique de sauvegarde régulièrement mise à jour. Cette dernière a pour objectif de définir des exigences en matière de sauvegarde de l'information, des logiciels et des systèmes.

Cette politique doit au moins intégrer les éléments suivants :

- la liste des données jugées vitales pour l'organisme et les serveurs concernés ;
- les différents types de sauvegarde (par exemple le mode hors ligne) ;
- la fréquence des sauvegardes ;
- la procédure d'administration et d'exécution des sauvegardes ;
- les informations de stockage et les restrictions d'accès aux sauvegardes ;
- les procédures de test de restauration ;
- la destruction des supports ayant contenu les sauvegardes.

Les tests de restauration peuvent être réalisés de plusieurs manières :

- systématique, par un ordonnanceur de tâches pour les applications importantes ;
- ponctuelle, en cas d'erreur sur les fichiers ;
- générale, pour une sauvegarde et restauration entières du système d'information.

/RENFORCÉ

Un fois cette politique de sauvegarde établie, il est souhaitable de planifier au moins une fois par an un exercice de restauration des données et de conserver une trace technique des résultats.

38 Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées

/RENFORCÉ

La réalisation d'audits réguliers (au moins une fois par an) du système d'information est essentielle car elle permet d'évaluer concrètement l'efficacité des mesures mises en œuvre et leur maintien dans le temps. Ces contrôles et audits permettent également de mesurer les écarts pouvant persister entre la règle et la pratique.

Ils peuvent être réalisés par d'éventuelles équipes d'audit internes ou par des sociétés externes spécialisées. Selon le périmètre à contrôler, des audits techniques et/ou organisationnels seront effectués par les professionnels mobilisés. Ces audits sont d'autant plus nécessaires que l'entité doit être conforme à des réglementations et obligations légales directement liées à ses activités.

À l'issue de ces audits, des actions correctives doivent être identifiées, leur application planifiée et des points de suivi organisés à intervalles réguliers. Pour une plus grande efficacité, des indicateurs sur l'état d'avancement du plan d'action pourront être intégrés dans un tableau de bord à l'adresse de la direction.

Si les audits de sécurité participent à la sécurité du système d'information en permettant de mettre en évidence d'éventuelles vulnérabilités, ils ne constituent jamais une preuve de leur absence et ne dispensent donc pas d'autres mesures de contrôle.

Les prestataires d'audit de la sécurité des systèmes d'information (PASSI) qualifiés par l'ANSSI délivrent des prestations d'audit d'architecture, de configuration, de code source, de tests d'intrusion et d'audit organisationnel et physique.

39 Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel

/STANDARD

Toute entité doit disposer d'un référent en sécurité des systèmes d'information qui sera soutenu par la direction ou par une instance décisionnelle spécialisée selon le niveau de maturité de la structure.

Ce référent devra être connu de tous les utilisateurs et sera le premier contact pour toutes les questions relatives à la sécurité des systèmes d'information :

- définition des règles à appliquer selon le contexte ;
- vérification de l'application des règles ;
- sensibilisation des utilisateurs et définition d'un plan de formation des acteurs informatiques ;
- centralisation et traitement des incidents de sécurité constatés ou remontés par les utilisateurs.

Ce référent devra être formé à la sécurité des systèmes d'information et à la gestion de crise.

Dans les entités les plus importantes, ce correspondant peut être désigné pour devenir le relais du RSSI. Il pourra par exemple signaler les doléances des utilisateurs et identifier les thématiques à aborder dans le cadre des sensibilisations, permettant ainsi d'élever le niveau de sécurité du système d'information au sein de l'organisme.

40 Définir une procédure de gestion des incidents de sécurité

/STANDARD

Le constat d'un comportement inhabituel de la part d'un poste de travail ou d'un serveur (connexion impossible, activité importante, activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, multiples alertes de l'antivirus, etc.) peut alerter sur une éventuelle intrusion.

Une mauvaise réaction en cas d'incident de sécurité peut faire empirer la situation et empêcher de traiter correctement le problème. Le bon réflexe est de déconnecter la machine du réseau, pour stopper l'attaque. En revanche, il faut la maintenir sous tension et ne pas la redémarrer, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque. Il faut ensuite prévenir la hiérarchie, ainsi que le référent en sécurité des systèmes d'information.

Celui-ci peut prendre contact avec un prestataire de réponse aux incidents de sécurité (PRIS) afin de faire réaliser les opérations techniques nécessaires (copie physique du disque, analyse de la mémoire, des journaux et d'éventuels codes malveillants, etc.) et de déterminer si d'autres éléments du système d'information ont été compromis. Il s'agira également d'élaborer la réponse à apporter afin de supprimer d'éventuels codes malveillants et accès dont disposerait l'attaquant et de procéder au changement des mots de passe compromis. Tout incident doit être consigné dans un registre centralisé. Une plainte pourra également être déposée auprès du service judiciaire compétent.

Les prestataires de réponse aux incidents de sécurité (PRIS) interviennent lorsqu'une concordance de signaux permet de soupçonner ou d'attester une activité informatique malveillante au sein d'un système d'information. La criticité de ces prestations engageant la pérennité des systèmes d'information, l'ANSSI a élaboré un référentiel dont l'objectif est d'apporter aux commanditaires de telles prestations les garanties nécessaires vis-à-vis de ces prestataires, tant en termes de compétence que de confiance.

X

POUR ALLER PLUS LOIN

41 Mener une analyse de risques formelle

/RENFORCÉ

Chaque entité évolue dans un environnement informationnel complexe qui lui est propre. Aussi, toute prise de position ou plan d'action impliquant la sécurité du système d'information doit être considéré à la lumière des risques pressentis par la direction. En effet, qu'il s'agisse de mesures organisationnelles ou techniques, leur mise en œuvre représente un coût pour l'entité qui nécessite de s'assurer qu'elles permettent de réduire au bon niveau un risque identifié.

Dans les cas les plus sensibles, l'analyse de risque peut remettre en cause certains choix passés. Ce peut notamment être le cas si la probabilité d'apparition d'un événement et ses conséquences potentielles s'avèrent critiques pour l'entité et qu'il n'existe aucune action préventive pour le maîtriser.

La démarche recommandée consiste, dans les grandes lignes, à définir le contexte, apprécier les risques et les traiter. L'évaluation de ces risques s'opère généralement selon deux axes : leur probabilité d'apparition et leur gravité. S'ensuit l'élaboration d'un plan de traitement du risque à faire valider par une autorité désignée à plus haut niveau.

Trois types d'approches peuvent être envisagés pour maîtriser les risques associés à son système d'information :

> le recours aux bonnes pratiques de sécurité informatique ;
> une analyse de risques systématique fondée sur les retours d'expérience des utilisateurs ;
> une gestion structurée des risques formalisée par une méthodologie dédiée.

Dans ce dernier cas, la méthode EBIOS référencée par l'ANSSI est recommandée. Elle permet d'exprimer les besoins de sécurité, d'identifier les objectifs de sécurité et de déterminer les exigences de sécurité.

La méthode d'analyse de risques EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires, constituant ainsi un outil complet de gestion des risques SSI.

42 Privilégier l'usage de produits et de services qualifiés par l'ANSSI

/RENFORCÉ

La qualification prononcée par l'ANSSI offre des garanties de sécurité et de confiance aux acheteurs de solutions listées dans les catalogues de produits et de prestataires de service qualifiés que publie l'agence.

Au-delà des entités soumises à réglementation, l'ANSSI encourage plus généralement l'ensemble des entreprises et administrations françaises à utiliser des produits qu'elle qualifie, seul gage d'une étude sérieuse et approfondie du fonctionnement technique de la solution et de son écosystème.

S'agissant des prestataires de service qualifiés, ce label permet de répondre aux enjeux et projets de cybersécurité pour l'ensemble du tissu économique français que l'ANSSI ne saurait adresser seule. Évalués sur des critères techniques et organisationnels, les prestataires qualifiés couvrent l'essentiel des métiers de la sécurité des systèmes d'information. Ainsi, en fonction de ses besoins et du maillage national, une entité pourra faire appel à un Prestataire d'audit de la sécurité des systèmes d'information (PASSI), un Prestataire de réponse aux incidents de sécurité (PRIS), un Prestataire de détection des incidents de sécurité (PDIS) ou à un prestataire de service d'informatique en nuage (SecNumCloud).

Catalogue des produits et prestataires de service qualifiés

I - Sensibiliser et former		STANDARD	RENFORCÉ
1	Former les équipes opérationnelles à la sécurité des systèmes d'information		
2	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique		
3	Maîtriser les risques de l'infogérance		

II - Connaitre le système d'information		STANDARD	RENFORCÉ
4	Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau		
5	Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour		
6	Organiser les procédures d'arrivée, de départ et de changement de fonction des utilisateurs		
7	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés		

III - Authentifier et contrôler les accès		STANDARD	RENFORCÉ
8	Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateur/administrateur		
9	Attribuer les bons droits sur les ressources sensibles du système d'information		
10	Définir et vérifier des règles de choix et de dimensionnement des mots de passe		
11	Protéger les mots de passe stockés sur les systèmes		
12	Changer les éléments d'authentification par défaut sur les équipements et services		
13	Privilégier lorsque c'est possible une authentification forte		

IV - Sécuriser les postes		STANDARD	RENFORCÉ
14	Mettre en place un niveau de sécurité minimal sur l'ensemble du parc informatique		
15	Se protéger des menaces relatives à l'utilisation de supports amovibles		
16	Utiliser un outil de gestion centralisée afin d'homogénéiser les politiques de sécurité		

17	Activer et configurer le pare-feu local des postes de travail		
18	Chiffrer les données sensibles transmises par voie Internet		

V - Sécuriser le réseau		STANDARD	RENFORCÉ
19	Segmenter le réseau et mettre en place un cloisonnement entre ces zones		
20	S'assurer de la sécurité des réseaux d'accès Wi-Fi et de la séparation des usages		
21	Utiliser des protocoles sécurisés dès qu'ils existent		
22	Mettre en place une passerelle d'accès sécurisé à Internet		
23	Cloisonner les services visibles depuis Internet du reste du système d'information		
24	Protéger sa messagerie professionnelle		
25	Sécuriser les interconnexions réseau dédiées avec les partenaires		
26	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques		

VI - Sécuriser l'administration		STANDARD	RENFORCÉ
27	Interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information		
28	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information		
29	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail		

VII - Gérer le nomadisme		STANDARD	RENFORCÉ
30	Prendre des mesures de sécurisation physique des terminaux nomades		
31	Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable		
32	Sécuriser la connexion réseau des postes utilisés en situation de nomadisme		
33	Adopter des politiques de sécurité dédiées aux terminaux mobiles		

VIII - Maintenir à jour le système d'information		STANDARD	RENFORCÉ
34	Définir une politique de mise à jour des composants du système d'information		
35	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles		

IX - Superviser, auditer, réagir		STANDARD	RENFORCÉ
36	Activer et configurer les journaux des composants les plus importants		
37	Définir et appliquer une politique de sauvegarde des composants critiques		
38	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées		
39	Désigner un référent en sécurité des systèmes d'information et le faire connaître auprès du personnel		
40	Définir une procédure de gestion des incidents de sécurité		

X - Pour aller plus loin		STANDARD	RENFORCÉ
41	Mener une analyse de risques formelle		
42	Privilégier l'usage de produits et de services qualifiés par l'ANSSI		

BIBLIOGRAPHIE

Guides et méthodes

ANSSI, *Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine*, guide, février 2015
www.ssi.gouv.fr/guide-bonnes-pratiques/

ANSSI, *Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS)*, méthode, janvier 2010
www.ssi.gouv.fr/ebios/

ANSSI, *Guide de l'externalisation – Maîtriser les risques de l'infogérance*, guide, décembre 2010
www.ssi.gouv.fr/externalisation/

ANSSI, *Maîtriser les risques de l'infogérance*, guide, décembre 2010
www.ssi.gouv.fr/infogerance/

ANSSI-CDSE, *Passeport de conseils aux voyageurs*, bonnes pratiques, janvier 2010
www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs/

Notes techniques

ANSSI, *Guide de définition d'une architecture de passerelle d'interconnexion sécurisée*, note technique, décembre 2011
www.ssi.gouv.fr/passerelle-interconnexion/

ANSSI, *Recommandations de sécurité relatives aux mots de passe*, note technique, juin 2012
www.ssi.gouv.fr/mots-de-passe/

ANSSI, *Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu*, note technique, mars 2013
www.ssi.gouv.fr/politique-filtrage-parefeu/

ANSSI, *Recommandations de sécurité relatives aux réseaux Wi-Fi*, note technique, septembre 2013
www.ssi.gouv.fr/nt-wifi/

ANSSI, *Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows*, note technique, décembre 2013
www.ssi.gouv.fr/windows-restrictions-logicielles/

ANSSI, *Recommandations de sécurité pour la mise en œuvre d'un système de journalisation*, note technique, décembre 2013
www.ssi.gouv.fr/journalisation/

ANSSI, *Recommandations de sécurité relatives à Active Directory*, note technique, septembre 2014
www.ssi.gouv.fr/Active-Directory/

ANSSI, *Recommandations relatives à l'administration sécurisée des systèmes d'information*, note technique, février 2015
www.ssi.gouv.fr/securisation-admin-si/

ANSSI, *Recommandations de sécurité relatives aux ordiphones*, note technique, juillet 2015
www.ssi.gouv.fr/securisation-ordiphones/

ANSSI, *Recommandations de sécurité relatives à IPsec pour la protection des flux réseau*, note technique, août 2015
www.ssi.gouv.fr/ipsec/

ANSSI, *Recommandations de configuration d'un système GNU/Linux*, note technique, janvier 2016
www.ssi.gouv.fr/reco-securite-systeme-linux/

Ressources en ligne

Site Web de l'ANSSI
Catalogue des produits et prestataires de service qualifiés
www.ssi.gouv.fr/qualifications/

Twitter
@ANSSI_FR
www.twitter.com/anssi_fr

CERT-FR
www.cert.ssi.gouv.fr

CNIL
www.cnil.fr

Références

Douglas Adams, *The Hitchhiker's Guide to the Galaxy* (ou *H2G2*), roman de science-fiction, 1979

Version 2.0 - Janvier 2017

20170125-1458

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51, boulevard de la Tour-Maubourg - 75700 PARIS 07 SP

www.ssi.gouv.fr / communication@ssi.gouv.fr