GUIDE D'HYGIÈNE INFORMATIQUE

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Table des matières

PRÉAMBULE

Les formidables développements de l'informatique et d'Internet ont révolutionné nos manières de vivre et de travailler.

La perte ou le vol de certaines informations ou l'indisponibilité de son système d'information peuvent avoir de lourdes conséquences pour l'entreprise : perte de confiance des clients, des partenaires, avantage pris par un concurrent, perte d'exploitation suite à une interruption de la production. Les communications de l'équipe dirigeante sont souvent une cible privilégiée.

Bien protéger les informations confidentielles confiées par des clients et des partenaires peut désormais créer un avantage concurrentiel. Plus encore, protéger ses données et son réseau informatique est crucial pour la survie de l'entreprise et sa compétitivité.

Si les erreurs humaines ou la malveillance d'un salarié peuvent être à l'origine d'un incident, les agressions externes sont de plus en plus fréquentes : attaque contre le site Internet de l'entreprise, programmes informatiques malveillants cachés dans des pièces jointes à des courriels ou dans des clés USB piégées, vol de mots de passe.

Il est de la responsabilité des dirigeants de vérifier que les mesures de protection adaptées sont mises en place et opérationnelles. Elles doivent faire l'objet d'une politique de sécurité écrite, comprise et connue de tous et dont l'application doit être régulièrement vérifiée par l'encadrement.

Parmi ces mesures, il existe des mesures techniques simples, qualifiées d'hygiène informatique car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.

La majeure partie des attaques informatiques sur lesquelles l'ANSSI est intervenue auraient pu être évitées si les mesures d'hygiène informatique décrites dans ce guide avaient été appliquées par les entreprises concernées.

S'adressant aux personnes en charge de la sécurité informatique, que ce soit un responsable de la sécurité des systèmes d'information (RSSI) ou toute autre personne qui remplit cette fonction, ce document présente les 40 règles d'hygiène informatique incontournables.

Elles ne prétendent pas avoir un caractère d'exhaustivité. Elles constituent cependant le socle minimum des règles à respecter pour protéger les informations d'une entreprise.

Ne pas les suivre expose l'entreprise à des risques d'incidents majeurs, susceptibles de mettre sa compétitivité, voire sa pérennité, en danger.

À DESTINATION DES RESPONSABLES INFORMATIQUES

Vous êtes responsable de la sécurité des systèmes d'information de votre organisation ou, plus simplement, c'est à vous que revient la responsabilité du bon fonctionnement de son informatique. Vous le savez, en quelques années, votre métier a évolué au rythme de l'arrivée des technologies de l'information qui irriguent désormais toutes les fonctions des entreprises, des administrations, des collectivités territoriales, comme de notre vie quotidienne. De nouveaux usages rendent également plus complexe la maîtrise des systèmes dont vous avez la charge.

Bases de données des clients, contrats commerciaux ou brevets, données de production, dossiers des usagers, démarches administratives, informations concernant un marché public sont désormais accessibles en ligne, le plus souvent via Internet à travers des postes de travail ou des téléphones mobiles.

Les conséquences qu'auraient pour votre organisation la perte ou le vol de certaines informations ou l'indisponibilité de son informatique peuvent être extrêmement lourdes. À l'inverse, bien protéger les informations confidentielles de l'entreprise ou celles confiées par des clients, des partenaires ou des fournisseurs génère la confiance et fluidifie l'activité.

Si les erreurs humaines ou la malveillance d'un employé peuvent parfois être à l'origine d'un incident, les agressions externes, à des fins d'espionnage voire de sabotage, sont aujourd'hui extrêmement fréquentes et discrètes.

Toutefois, de nombreuses attaques informatiques, traitées par l'agence nationale de sécurité des systèmes d'information (ANSSI), auraient pu être évitées si des mesures techniques essentielles avaient été appliquées par les organisations victimes.

Certaines de ces mesures peuvent être qualifiées de « règles élémentaires d'hygiène informatique ». Ne pas les suivre expose inutilement votre organisation à des risques d'incidents majeurs, susceptibles de mettre son fonctionnement ou sa compétitivité en danger, voire d'entraîner l'arrêt de son activité.

Ce guide s'adresse à vous. Il vous présente les 40 règles d'hygiène informatique essentielles pour assurer la sécurité de votre système d'information et le moyen de les mettre en œuvre. Non exhaustives, ces règles représentent cependant le socle minimum à respecter pour protéger les informations de votre organisation.

Une fois ces règles partagées et appliquées, vous aurez accompli une part importante de votre mission : permettre à votre organisation d'interagir avec ses fournisseurs et ses partenaires, de servir ses clients, en respectant l'intégrité et la confidentialité des informations qui les concernent.

Ce document se concentre sur les systèmes de bureautique classiques. Bien qu'un certain nombre des recommandations décrites ici s'appliquent également aux systèmes industriels, l'ANSSI a publié un guide spécifique pour assurer la sécurité des systèmes de ce type[1].

1 Voir sur le site de l'ANSSI : www.ssi.gouv.fr/systemesindustriels.

I - CONNAÎTRE LE SYSTÈME D'INFORMATION ET SES UTILISATEURS

La connaissance de son propre système d'information est un préalable important à sa sécurisation. En effet, si le système d'information comprend un équipement régulièrement omis des inventaires, cet équipement, qui deviendra rapidement obsolète, sera une cible de choix pour un attaquant.

Règle 1

Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour.

L'élaboration d'une cartographie du système d'information est le premier pas vers une meilleure connaissance du système d'information. Elle permettra d'élaborer plus facilement des mesures de sécurité adaptées au système, de garantir qu'aucun équipement n'est oublié lors de l'application d'une mesure de sécurité et de faciliter la réaction en cas d'incident.

Cette cartographie doit au minimum comprendre les éléments suivants :

- liste des ressources matérielles (avec leur modèle) et logicielles (avec leur version) utilisées. Il convient bien entendu d'être le plus précis possible. Pour entamer la démarche, l'établissement d'une liste des machines déployées associées à leurs attributaires et à leurs paramètres techniques (adresse IP, adresse MAC) d'une part, et des logiciels principaux déployés sur ces postes (suite bureautique, visionneuse PDF, navigateur, client de messagerie) avec leurs versions peut être envisagé. Par ailleurs, les postes d'administration doivent faire partie du périmètre de la cartographie. Plus le parc est homogène, plus l'établissement et le maintien à jour d'une telle liste sont aisés ;
- architecture réseau sur laquelle sont identifiés les points névralgiques (connexions externes[1], serveurs hébergeant des données ou des fonctions sensibles, etc.).

1 **Inventorier en particulier tous les accès Internet du système d'information et toutes les interconnexions avec des réseaux partenaires (fournisseurs, partenaires commerciaux, etc.). Cet inventaire doit être exhaustif. Il doit comprendre les accès ADSL éventuellement mis en place pour les besoins spécifiques des utilisateurs ainsi que les liaisons spécialisées.**

Une fois cette cartographie établie, elle doit être maintenue à jour et enrichie, notamment avec des éléments liés aux protocoles mis en œuvre (matrices de flux).

Cette cartographie ne doit idéalement pas être stockée sur le réseau qu'elle représente, car il s'agit de l'un des éléments que l'attaquant va rechercher en premier lieu en cas d'intrusion réussie.

Règle 2

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

A minima, il est important de disposer de la liste :

- des utilisateurs qui disposent d'un compte administrateur (ou de privilèges supérieurs à ceux d'un utilisateur standard) sur le système d'information ;
- des utilisateurs qui disposent de privilèges suffisants pour accéder aux répertoires de travail des dirigeants ou, *a fortiori*, de l'ensemble des utilisateurs ;
- des utilisateurs qui disposent d'un poste non administré par le service informatique et donc non géré selon la politique de sécurité générale de l'organisme.

Cette liste doit bien entendu être maintenue à jour.

Par ailleurs, il est souhaitable de disposer de la liste des utilisateurs qui disposent de privilèges suffisants pour lire la messagerie des dirigeants de la société ou *a fortiori* de l'ensemble des utilisateurs. L'établissement de la liste des personnes ayant réellement accès à ces informations est cependant parfois extrêmement difficile. Si la liste ne peut être établie de manière fiable, une journalisation des accès aux boîtes à lettres et une vérification périodique de la liste des personnes ayant consulté les boîtes à lettres les plus sensibles devraient être réalisée (voir règle 26).

Sur un système Windows, la plupart de ces informations peuvent être obtenues par l'analyse de la configuration de l'*Active Directory*. Le document *Audit des permissions en environnement Active Directory*[2] disponible sur le site de l'ANSSI

2 Voir sur le site Internet de l'ANSSI : http://www.ssi.gouv.fr/Active-Directory.

précise un ensemble de méthodes permettant d'en réaliser l'inventaire.

Il est de plus très fortement recommandé d'utiliser une nomenclature claire pour les noms de comptes (faire systématiquement précéder les noms de comptes de service par le préfixe SRV, les comptes d'administration du préfixe ADM).

Rédiger et appliquer des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires…).

Ces procédures sont destinées à garantir que les droits octroyés sur le système d'information sont appliqués au plus juste. Notamment, il est important que l'ensemble des droits affectés à une personne soient révoqués lors de son départ. Les procédures doivent décrire *a minima* :

- la gestion (création / destruction) des comptes informatiques (et des boîtes à lettres associées) et l'attribution des droits associés à ces comptes sur le système d'information, y compris pour les partenaires et les prestataires externes ;
- la gestion des accès aux locaux (perception et restitution des cartes d'accès aux locaux notamment) ;
- la gestion des équipements mobiles ;
- la gestion des documents sensibles (détention, éventuelles autorisations de sortie) ;
- la gestion du contrôle des habilitations du personnel.

Il est important de bien gérer les mutations de personnel, soit en les traitant comme un départ suivi d'une arrivée soit en définissant une procédure adaptée. On observe fréquemment une inflation des privilèges associés à certains comptes utilisateur du fait de mouvements internes qui conduisent à l'ouverture de nouveaux droits sans suppression de ceux devenus inutiles.

II - MAÎTRISER LE RÉSEAU

Règle 4

Limiter le nombre d'accès Internet de l'entreprise au strict nécessaire.

Il convient de connaître précisément les points d'accès à Internet (box ADSL, etc.) et les interconnexions avec des réseaux partenaires et de les limiter au strict nécessaire de manière à pouvoir plus facilement centraliser et rendre homogène la surveillance des échanges.

Règle 5

Interdire la connexion d'équipements personnels au système d'information de l'organisme.

La connexion des équipements personnels ne peut être envisagée que sur des réseaux ne contenant strictement aucune information sensible. Les équipements personnels (assistants personnels, tablettes, smartphones, lecteurs MP3, clés USB) sont en effet difficilement maîtrisables par l'organisme dans la mesure où ce sont les utilisateurs eux-mêmes qui décident du niveau de sécurité de leurs équipements. Les mesures de sécurité en vigueur au sein d'un établissement ou d'une entreprise ne peuvent donc, par essence, pas s'appliquer à ce type d'équipement.

Cette règle est le plus souvent perçue comme une contrainte inacceptable voire rétrograde par de très nombreux utilisateurs. Cependant, y déroger facilite grandement le travail d'un attaquant en fragilisant le réseau de l'entreprise. En effet, sur une centaine d'équipements personnels connectés au réseau d'une entreprise, on estime statistiquement qu'au minimum dix d'entre eux sont compromis par un code malveillant générique (sans parler d'attaque ciblée).

Il est donc important d'interdire ou d'empêcher leur connexion au système d'information de l'entreprise. Cette interdiction est d'abord organisationnelle : même si aucune règle technique n'empêche leur connexion, il convient d'inciter les utilisateurs à ne pas recourir à de telles pratiques par exemple au moyen de la charte d'utilisation des moyens informatiques.

Cette interdiction doit dans la mesure du possible être complétée par des mesures techniques, dont la mise en œuvre peut toutefois s'avérer plus complexe (contrôle systématique d'accès au réseau, désactivation des ports USB).

Lorsque le travail à distance est nécessaire, l'organisme doit fournir des moyens professionnels pour permettre de tels usages. Le transfert de messages des messageries professionnelles vers des messageries personnelles doit être explicitement interdit.

III - METTRE À NIVEAU LES LOGICIELS

Chaque jour, des vulnérabilités sont mises en évidence dans de très nombreux logiciels largement utilisés. Quelques heures sont parfois suffisantes pour que des codes malveillants exploitant ces vulnérabilités commencent à circuler sur Internet. Il est donc très important d'utiliser en priorité des technologies pérennes, dont le support est assuré, d'éviter les technologies non maîtrisées en interne et de respecter les recommandations du présent chapitre.

Règle 6

Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés et se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.

Il est primordial de déterminer comment les composants logiciels utilisés par l'entreprise peuvent être mis à jour. Si un composant ne peut être mis à jour, il ne doit pas être utilisé (voir la règle 7 pour la gestion des exceptions en la matière). Par ailleurs, les mises à jour (comme les logiciels) ne doivent être téléchargées que depuis des sites de confiance (le site de leur éditeur généralement).

Il est recommandé de traiter en priorité les composants de base (système d'exploitation, suite bureautique, navigateur et outils nécessaires à la navigation – tels que la machine virtuelle Java ou le lecteur Flash, visionneuses de document) puis de compléter l'inventaire avec l'ensemble des autres composants logiciels et d'intégrer ces éléments à la cartographie.

Il est par ailleurs nécessaire d'inventorier et de suivre les sources d'information susceptibles de remonter des vulnérabilités sur les composants identifiés et de diffuser des mises à jour (site des éditeurs des logiciels considérés, sites des CERT).

Règle 7

Définir une politique de mise à jour et l'appliquer strictement.

Cette politique devra comprendre :

- les éléments à mettre à jour ;
- les responsabilités des différents acteurs dans cette mise à jour ;
- les moyens de récupération et de qualification des mises à jour.

Elle pourra prendre la forme d'un simple tableau comprenant ces éléments.

Lorsqu'il en existe, il convient d'utiliser un outil dédié (par exemple WSUS en environnement Microsoft) permettant d'appliquer les mises à jour de manière homogène sur l'ensemble du parc. D'une manière générale, une qualification des mises à jour en termes d'impact sur le fonctionnement du système doit être réalisée avant application.

Il est impératif, en vertu de la règle 6 ci-dessus, de n'exclure aucun composant, et *a fortiori* aucun poste, de la politique de mise à jour.

Cependant, il est malheureusement fréquent que des services informatiques maintiennent en fonctionnement des systèmes obsolètes qui ne sont plus supportés par leurs fabricants en raison d'une adhérence particulière des applications à ce système. Dans ce cas, il est primordial d'isoler ces systèmes :

- au niveau du réseau, à l'aide d'un filtrage très strict n'autorisant qu'un accès aux applications nécessaires ;
- au niveau de l'authentification, en n'utilisant aucun mot de passe (système et logiciel) commun avec le reste du système d'information ;
- au niveau des applications, en s'assurant que ces systèmes n'utilisent pas de ressources partagées avec le reste du système d'information.

Par ailleurs, les équipements isolés (déconnectés du réseau) ne doivent pas être exclus de la politique de mise à jour. Pour ces systèmes, une mise à jour manuelle s'impose.

IV - AUTHENTIFIER L'UTILISATEUR

Les mots de passe constituent souvent le talon d'Achille des systèmes d'information. En effet, si les organismes définissent relativement fréquemment une politique de mots de passe, il est rare qu'elle soit effectivement appliquée de manière homogène sur l'ensemble du parc informatique.

Règle 8

Identifier nommément chaque personne ayant accès au système.

Cette règle dont l'objet est de supprimer les comptes et accès génériques et anonymes est destinée à faciliter l'attribution d'une action sur le système. Cela sera particulièrement utile en cas d'incident.

Bien entendu, cette règle n'interdit pas de conserver des comptes techniques (dits de service) non attribués à une personne physique mais reliés à un service, un métier ou une application (par exemple utilisateur « *apache* » pour un serveur web). Ces comptes doivent cependant être gérés avec une politique au moins aussi stricte que celle des comptes nominatifs.

Règle 9

Définir des règles de choix et de dimensionnement des mots de passe.

On trouvera les bonnes pratiques en matière de choix et de dimensionnement des mots de passe dans le document de l'ANSSI, *Recommandations de sécurité relatives aux mots de passe*[3]. Parmi ces règles, les plus critiques sont de sensibiliser les utilisateurs aux risques liés au choix d'un mot de passe qui puisse se deviner trop facilement, et à la réutilisation de mots de passe en particulier entre messageries personnelles et professionnelles.

3 Voir http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/mot-de-passe.html.

Règle 10

Mettre en place des moyens techniques permettant de faire respecter les règles relatives à l'authentification.

Les moyens permettant de faire respecter la politique en matière d'authentification et de mots de passe pourront être :

- le blocage des comptes tous les 6 mois tant que le mot de passe n'a pas été changé ;
- le blocage de toute configuration du poste qui permettrait le démarrage du poste dans un mode « sans mot de passe » (*autologon*) ou depuis un compte invité ;
- la vérification que les mots de passe choisis ne sont pas faciles à retrouver.

Certains outils permettent par ailleurs nativement de vérifier au moment du changement de mot de passe que le nouveau mot de passe choisi n'est pas trivialement simple à retrouver à partir de l'ancien mot de passe. Bien que l'objectif de ce type d'outil soit louable (il est souvent facile de deviner le nouveau mot de passe d'un utilisateur à partir de la connaissance de ses autres mots de passe), il est fortement déconseillé de les utiliser sauf lorsqu'ils sont bien maîtrisés car ils peuvent nécessiter de conserver un historique des anciens mots de passe.

Règle 11

Ne pas conserver les mots de passe en clair dans des fichiers sur les systèmes informatiques.

Par souci de simplicité, les utilisateurs ou les administrateurs écrivent fréquemment leurs mots de passe en clair dans des fichiers stockés sur leurs postes informatiques ou se les envoient par courriel. Ces pratiques sont à proscrire. Les mots de passe ou les éléments secrets stockés sur les machines des utilisateurs sont des éléments recherchés et exploités en priorité par les attaquants.

Il est en outre important de ne pas utiliser de mécanismes automatiques de sauvegarde des mots de passe (bouton «toujours se souvenir du mot de passe» d'un navigateur par exemple). Si le nombre de mots de passe impose de recourir à une solution de stockage centralisé, il faut recourir à un système dont la sécurité a été expertisée. L'ANSSI a certifié des produits permettant ce type d'usage[4].

4 http://www.ssi.gouv.fr/fr/produits-et-prestataires/.

Règle 12

Renouveler systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).

Les éléments par défaut sont systématiquement connus des attaquants. Par ailleurs, ils sont bien souvent triviaux (mot de passe identique à l'identifiant correspondant, mot de passe partagé entre plusieurs équipements d'une même gamme, etc.). Ils doivent donc être changés. Si la modification n'est pas possible (certificat « en dur » dans un équipement par exemple), ce problème critique doit être signalé au constructeur afin qu'il corrige au plus vite cette vulnérabilité.

Règle 13

Privilégier lorsque c'est possible une authentification forte par carte à puce.

Il est fortement recommandé de mettre en œuvre une authentification forte reposant sur l'emploi d'une carte à puce dont l'utilisation nécessite la connaissance d'un code PIN (voir annexe B.3 du référentiel général de sécurité[5]).

La mise en place d'un mécanisme de contrôle d'accès par carte à puce sur un système n'en disposant pas est cependant plus longue et coûteuse que la mise en œuvre des autres règles décrites dans ce document.

5 http://www.ssi.gouv.fr/rgs.

V - SÉCURISER LES ÉQUIPEMENTS TERMINAUX

Si, il y a encore quelques années, les attaquants ciblaient en priorité les serveurs, l'attaque d'un poste client est aujourd'hui l'un des moyens les plus simples pour pénétrer sur un réseau. En effet, il n'est pas rare que les postes clients soient moins bien sécurisés et surtout moins bien supervisés que les serveurs.

Règle 14

Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique.

Il est en particulier impératif, au minimum, de désactiver les services inutiles et de restreindre les privilèges des comptes utilisateurs. L'utilisation d'un pare-feu personnel configuré au minimum pour bloquer les connexions entrantes non sollicitées sur chaque poste client est généralement indispensable. Sur les systèmes qui le permettent (serveurs ou postes clients sous Linux par exemple), le durcissement du système d'exploitation par l'ajout de composants optionnels de sécurité (GRSec, PaX etc.) doit être envisagé.

Par ailleurs, le BIOS des machines doit être verrouillé avec un mot de passe non trivial et le démarrage sur supports amovibles ou via le réseau (Wake On LAN) désactivé.

Au niveau applicatif, il convient de configurer le plus finement possible les clients de réception de courriel (forcer l'émission et la réception de courrier en texte brut et non en HTML est par exemple une bonne pratique), les navigateurs (bloquer par défaut certains contenus et n'activer le support qu'au cas par cas par exemple), ou les suites de bureautique (désactiver les possibilités d'exécution des macros).

Concernant ce dernier point, il est à noter que le blocage de certains contenus (javascript, flash), même s'il est primordial du point de vue de la sécurité est souvent perçu comme difficile voire impossible car l'accès à l'information nécessite l'utilisation de ces technologies. Il est cependant important qu'au minimum, ces technologies soient désactivées sur les machines sur lesquelles leur utilisation n'est pas strictement nécessaire.

Règle 15

Interdire techniquement la connexion des supports amovibles sauf si cela est strictement nécessaire ; désactiver l'exécution des autoruns depuis de tels supports.

Les supports amovibles sont un moyen privilégié de propagation des codes malveillants et d'exfiltration de données. Il convient donc d'essayer d'en limiter au maximum l'usage. Il n'est souvent pas réaliste d'interdire complètement la connexion de supports amovibles sur l'ensemble des machines de l'entreprise. La bonne démarche est d'identifier les machines sur lesquelles la connexion de support amovibles est nécessaire, de n'autoriser la connexion que sur celles-ci et de reprendre fréquemment cette liste dans une optique de minimisation du nombre de machines qui y figurent.

De nombreuses organisations privilégient l'utilisation de stations blanches (ou « sas d'accès ») par lesquelles doivent passer l'ensemble des supports amovibles avant d'être connectés au système de l'entreprise. Si l'objectif est louable (effectuer un contrôle de l'innocuité des supports avant leur connexion), ces stations deviennent rapidement un point névralgique du système d'information (elles sont accessibles à tous les utilisateurs, elles sont elles-mêmes très exposées). Leur usage ne doit être envisagé que si elles peuvent être maîtrisées.

En tout état de cause, l'exécution automatique de code depuis des supports amovibles (*autorun*) doit être systématiquement interdite techniquement.

Par ailleurs, il est possible sur les systèmes Microsoft à partir de Windows XP, de restreindre la possibilité d'exécuter des programmes selon divers critères, grâce aux stratégies de restriction logicielle (Software Restriction Policies). Une telle politique peut être mise en œuvre dans le but de limiter le risque d'importation involontaire de virus, en particulier par clé USB.

Règle 16

Utiliser un outil de gestion de parc informatique permettant de déployer des politiques de sécurité et les mises à jour sur les équipements.

L'utilisation d'un outil de gestion de parc est primordiale pour assurer le suivi des postes sur le réseau.

Il est nécessaire d'inclure un maximum d'équipements informatiques dans le périmètre des équipements gérés par l'outil en question.

Règle 17

Gérer les terminaux nomades selon une politique de sécurité au moins aussi stricte que celle des postes fixes.

En cas de disparité de traitement entre les terminaux nomades et les postes fixes, le niveau réel de sécurité du réseau est celui du maillon le plus faible.

Les postes nomades doivent donc bénéficier au moins des mêmes mesures de sécurité que les postes fixes (mises à jour, restriction de privilèges etc.). Les conditions d'utilisation des postes nomades imposent de plus, souvent, le renforcement de certaines fonctions de sécurité (chiffrement de disque, authentification renforcée, voir règle 19) mais la mise en place de telles fonctions sur les postes fixes est également une bonne pratique au titre de la défense en profondeur.

Règle 18

Interdire dans tous les cas où cela est possible les connexions à distance sur les postes clients.

Dans les cas où l'application de cette règle n'est pas possible, respecter strictement les principes décrits dans le document technique *Recommandations de sécurité relatives* à la téléassistance[6].

Règle 19

Chiffrer les données sensibles, en particulier sur les postes nomades et les supports potentiellement perdables.

La perte ou le vol d'un équipement (ou d'un support) mobile ou nomade peut être lourd de conséquences pour l'entreprise : en l'absence de chiffrement, les données stockées sur le terminal (patrimoine technologique de l'entreprise, base de données client) seront en effet compromises, et ce même si le terminal est éteint ou si la session utilisateur est fermée. Il est donc important de chiffrer les données sensibles. Plusieurs produits de chiffrement de disques ou de partitions (ou supports chiffrants) ont été qualifiés par l'ANSSI[7]. Il convient de les utiliser en priorité. La qualification par l'ANSSI garantit la robustesse des mécanismes cryptographiques mis en œuvre.

Le chiffrement peut être réalisé sur l'ensemble du système (on parle de chiffrement intégral), sur un sous-ensemble du système (chiffrement de partitions) ou sur les fichiers les plus sensibles. Les mécanismes de chiffrement intégral de disque sont les plus efficaces du point de vue de la sécurité et ne nécessitent pas pour l'utilisateur d'identifier les fichiers à chiffrer. Dans les cas où la mise en œuvre de ce type de système de chiffrement s'avère trop complexe (par exemple pour une organisation de petite taille), il est impératif de mettre à disposition des utilisateurs un système de chiffrement de partitions.

6 Voir sur le site de l'ANSSI : http://www.ssi.gouv.fr/IMG/pdf/NP_Teleassistance_NoteTech.pdf.

7 Voir sur le site Internet de l'ANSSI : http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/ .

VI - SÉCURISER L'INTÉRIEUR DU RÉSEAU

Il est important de ne pas se contenter de mettre en place des mesures périmétriques (pare-feux, serveurs mandataires). En effet, si ces dernières sont indispensables (voir Section VII), il existe de nombreux moyens pour un attaquant de les contourner. Il est donc indispensable que le réseau se protège contre un attaquant qui aurait déjà contourné ces mesures de défense périmétriques.

Les services d'annuaire (*Active Directory*, *Lightweight Directory Access Protocol* - LDAP) permettant d'attribuer à chaque utilisateur des droits sur un système d'information sont par ailleurs des éléments cruciaux qui constituent une cible de choix pour les attaquants et dont il convient de vérifier fréquemment l'intégrité.

Règle 20

Auditer ou faire auditer fréquemment la configuration de l'annuaire central (*Active Directory* en environnement Windows ou annuaire LDAP par exemple)

Il est recommandé de suivre les règles énoncées dans l'article *Audit des permissions en environnement Active Directory*[8]. Il convient notamment de vérifier à intervalles réguliers si les droits d'accès aux données des personnes clés de l'entreprise (dirigeants notamment) sont correctement positionnés.

8 Voir http://www.ssi.gouv.fr/Active-Directory.

Règle 21

Mettre en place des réseaux cloisonnés. Pour les postes ou les serveurs contenant des informations importantes pour la vie de l'entreprise, créer un sous-réseau protégé par une passerelle d'interconnexion spécifique.

Lorsque le réseau est « à plat »[9], la compromission d'un contrôleur de domaine entraîne systématiquement la compromission de l'ensemble du réseau.

Il est important de prendre en compte cette règle en amont dès la conception du réseau. En effet, en fonction de l'étendue du réseau et de sa complexité, il sera souvent très difficile *a posteriori* de cloisonner le réseau. Pour les réseaux dont le cloisonnement ne serait pas aisé, il est recommandé :

- de prendre en compte les besoins de cloisonnement dans toute nouvelle extension du réseau ;
- d'élaborer un plan de réflexion sur l'architecture du réseau qui sort du cadre strict de l'hygiène informatique.

Règle 22

Éviter l'usage d'infrastructures sans fil (Wifi). Si l'usage de ces technologies ne peut être évité, cloisonner le réseau d'accès Wifi du reste du système d'information.

L'usage des technologies sans fil au sein d'un réseau n'est pas conseillé (faibles garanties en matière de disponibilité, difficulté de définition d'une architecture d'accès sécurisée à faible coût, etc.).

Si de telles technologies doivent être employées, la segmentation de l'architecture réseau doit permettre de limiter les conséquences d'une intrusion depuis la voie radio à un périmètre déterminé. Le cloisonnement du réseau d'accès Wifi du reste du réseau est fortement conseillé : l'interconnexion au réseau principal doit se

9 Un réseau « à plat » est un réseau ne mettant en œuvre aucun mécanisme de cloisonnement réseau en interne. Chaque machine du réseau a donc la possibilité d'accéder à n'importe quelle autre machine du réseau.

faire au travers d'une passerelle maîtrisée permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires. La conception d'un tel réseau d'accès sort du cadre des mesures élémentaires d'hygiène informatique.

De plus, il est important d'avoir prioritairement recours à un chiffrement des réseaux Wifi reposant sur WPA Entreprise (EAP-TLS avec chiffrement WPA2 CCMP) qui permet l'authentification des machines par certificats clients des machines accédant au réseau. Les mécanismes de protection basés sur une clé partagée doivent être proscrits dès lors que des prestataires externes ou un trop grand nombre d'utilisateurs doivent être amenés à accéder à ce réseau Wifi.

Il convient également d'éviter le recours aux technologies CPL (Courants Porteurs en Ligne) sans avoir recours à des mécanismes de protection équivalents à ceux recommandés pour les technologies sans fil. Le périmètre couvert par le réseau CPL est en effet difficile à définir précisément.

Utiliser systématiquement des applications et des protocoles sécurisés.

L'utilisation de protocoles sécurisés, y compris sur le réseau interne, contribue à la défense en profondeur et complique la tâche d'un attaquant qui aurait déjà compromis une machine sur le réseau et qui chercherait à étendre son emprise sur ce dernier.

Les protocoles non sécurisés (telnet, FTP, POP, SMTP, HTTP) sont en règle générale à proscrire sur le réseau de l'entreprise, et à remplacer par leurs équivalents sécurisés (SSH, SFTP, POPS, SMTPS, HTTPS, etc.).

Par ailleurs, il est important que les applications métier soient développées en considérant les risques de sécurité. Leur adhérence à une technologie particulière (version donnée d'un système d'exploitation ou d'une machine virtuelle Java typiquement) doit être réduite, de manière à ne pas limiter les capacités de maintien en conditions de sécurité et de mises à jour de ces applications.

VII - PROTÉGER LE RÉSEAU INTERNE DE L'INTERNET

Si certaines attaques peuvent être d'origine interne, l'un des moyens principaux d'attaque constatés par l'ANSSI est l'infection suite à la connexion sur un site Internet compromis. Il est donc important, en complément des mesures de protection du réseau interne, dont la limitation du nombre d'interconnexions présentées plus haut dans ce document, de mettre en place des mesures de défense périmétriques spécifiques.

Règle 24

Sécuriser les passerelles d'interconnexion avec Internet.

Il faut pour cela mettre en place des services de sécurité correctement configurés (par exemple, conformes aux recommandations du document *Définition d'une architecture de passerelle d'interconnexion sécurisée*[10]) permettant un cloisonnement entre l'accès Internet, la zone de service (DMZ) et le réseau interne.

Règle 25

Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis l'Internet.

De nombreux équipements comportent des interfaces d'administration (par exemple via un serveur web). Certaines de ces interfaces sont accessibles par défaut et ne seront donc désactivées qu'en cas d'action explicite de l'administrateur de l'équipement. Ces interfaces sont souvent exploitées par les attaquants dans le cadre d'une intrusion, *a fortiori* si elles sont exposées sur Internet. Plusieurs milliers d'entreprises exposent sur Internet ce type d'interface, le plus souvent sans en être conscientes.

Cette règle concerne les imprimantes, les serveurs, les routeurs, les commutateurs réseau ainsi que les équipements industriels ou de supervision.

10 Voir http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-reseaux/definition-d-une-architecture-de-passerelle-d-interconnexion-securisee.html.

VIII - SURVEILLER LES SYSTÈMES

La plupart des mesures décrites jusqu'ici sont de nature préventive et destinées à réduire le risque d'exploitation par un attaquant d'une des vulnérabilités du système. La mise en place de mesures préventives ne dispense jamais d'une supervision du système lors de son exploitation. Cette supervision doit respecter les règles proposées dans ce chapitre.

Définir concrètement les objectifs de la supervision des systèmes et des réseaux.

Dans la majeure partie des cas, les événements suivants doivent générer une alerte qui doit impérativement être traitée dans les 24 heures :

- connexion d'un utilisateur hors de ses horaires habituels de travail ou pendant une période d'absence déclarée ;
- transfert massif de données vers l'extérieur de l'entreprise ;
- tentatives de connexions successives ou répétées sur un service ;
- tentatives de connexion sur un compte non actif ;
- tentatives de contournement de la politique de sécurité (utilisation d'un service interdit, connexion non autorisée à un service, etc.).

Règle 27

Définir les modalités d'analyse des événements journalisés.

Il est primordial de définir également les procédures de vérification des journaux qui permettront de générer une alerte dès lors que l'un des objectifs identifiés n'est pas rempli. Ces procédures devront garantir que les journaux sont fréquemment analysés.

Outre les éléments mentionnés dans la règle 26, l'analyse des journaux pourra notamment se concentrer sur les points suivants :

- analyse de la liste des accès aux comptes de messagerie des personnes-clé de l'entreprise ;
- analyse des accès aux machines ou aux ressources sensibles de l'entreprise.

Afin de faciliter la vérification des journaux, il est primordial que les machines soient synchronisées sur la même horloge.

IX - SÉCURISER L'ADMINISTRATION DU RÉSEAU

Dans de nombreux cas traités par l'ANSSI, les attaquants ont pris le contrôle complet, via internet, des postes des administrateurs ou de comptes d'administration afin de bénéficier des privilèges les plus élevés sur le système.

Interdire tout accès à Internet depuis les comptes d'administration.

Cette interdiction s'applique en particulier aux machines des administrateurs du système. Cette règle est généralement mal acceptée par les utilisateurs car elle peut générer des contraintes d'exploitation (obligation d'utiliser des comptes distincts en fonction des actions réalisées). Le poids de cette contrainte peut être notablement allégé en équipant les administrateurs de deux postes distincts, afin de leur permettre par exemple de consulter la documentation sur le site d'un constructeur avec un poste (en utilisant leur compte non privilégié) tout en administrant l'équipement concerné sur l'autre (avec leur compte d'administrateur). Cela facilite en outre l'application de la règle 29.

Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.

Le cloisonnement du réseau d'administration vis-à-vis du réseau de travail des utilisateurs est impératif. Il est recommandé (en fonction des capacités de l'organisme) :

- de privilégier un cloisonnement physique des réseaux dès que cela est possible ;
- à défaut, mettre en œuvre un cloisonnement logique cryptographique basé

sur la mise en place de tunnels IPsec reposant sur un produit qualifié par l'ANSSI. L'intégrité et la confidentialité des informations véhiculées sur le réseau d'administration sont ainsi assurées vis-à-vis du réseau de travail courant de l'entreprise ;

- *a minima*, de mettre en œuvre un cloisonnement logique par VLAN.

Les postes d'administration étant particulièrement critiques, ils doivent être suivis en priorité. La mise à jour des postes du réseau d'administration est primordiale.

Règle 30

Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception.

De nombreux utilisateurs, y compris au sommet des hiérarchies, sont tentés de demander à leur service informatique de pouvoir disposer de privilèges plus importants sur leurs machines (pouvoir installer des logiciels, pouvoir connecter des équipements personnels, etc.). De tels usages sont cependant excessivement dangereux et sont susceptibles de mettre en danger le réseau dans son ensemble.

Règle 31

N'autoriser l'accès à distance au réseau d'entreprise, y compris pour l'administration du réseau, que depuis des postes de l'entreprise qui mettent en œuvre des mécanismes d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes.

Privilégier pour cela des mécanismes d'authentification et des moyens de protection de l'intégrité et de la confidentialité qualifiés par l'ANSSI.

X - CONTRÔLER L'ACCÈS AUX LOCAUX ET LA SÉCURITÉ PHYSIQUE

La sécurité du système de contrôle d'accès aux locaux est bien souvent critique pour la sécurité d'une entreprise. En effet, dès lors qu'un attaquant parvient à obtenir un accès au réseau interne de l'entreprise, les mesures de sécurité périmétriques mises en place deviennent inefficaces. La mise en adéquation des mesures de sécurité physique avec les besoins de protection des systèmes d'information est d'autant plus complexe que les équipes en charge de ces deux aspects sont bien souvent distinctes. Les responsabilités de chacune doivent être clarifiées et formalisées.

Règle 32

Utiliser impérativement des mécanismes robustes de contrôle d'accès aux locaux.

Le mécanisme de contrôle d'accès mis en œuvre doit être à l'état de l'art afin d'assurer qu'il ne puisse pas être contourné aisément par un attaquant. L'ANSSI a publié un guide permettant d'assister les entreprises dans la sélection d'un mécanisme de contrôle d'accès robuste[11].

Règle 33

Protéger rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme.

Les règles suivantes doivent être appliquées :

- récupérer systématiquement les clés ou les badges d'un employé à son départ définitif de l'entreprise ;
- changer fréquemment les codes de l'alarme de l'entreprise ;

11 Voir sur le site Internet de l'ANSSI : http://www.ssi.gouv.fr/sans-contact.

- ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs sauf s'il est possible de tracer ces accès et de les restreindre techniquement à des plages horaires données.

Règle 34

Ne pas laisser de prises d'accès au réseau interne accessibles dans les endroits ouverts au public.

Ces endroits publics peuvent être des salles d'attente, des placards ou des couloirs par exemple. Les attaquants peuvent par exemple récupérer un accès au réseau de l'entreprise en connectant une machine d'attaque en lieu et place des équipements suivants, dès lors que ceux-ci sont connectés au réseau :

- imprimantes ou photocopieurs multifonctions entreposés dans un couloir ;
- écrans d'affichage diffusant des flux d'information ;
- caméras de surveillance ;
- téléphones :
- prises réseau dans une salle d'attente.

Par ailleurs, les chemins de câbles du réseau interne ne devraient pas non plus être accessibles dans les lieux publics.

S'il est toutefois nécessaire de rendre ponctuellement accessible le réseau depuis une prise située dans un espace public (pour une présentation par exemple), la prise doit être brassée pour l'occasion et débrassée dès que possible.

Règle 35

Définir les règles d'utilisation des imprimantes et des photocopieuses.

Les règles suivantes peuvent être définies :

- utiliser des imprimantes disposant d'un mécanisme d'impression nécessitant la présence physique du demandeur pour démarrer l'impression ;
- détruire en fin de journée les documents oubliés sur l'imprimante ou la photocopieuse ;
- broyer les documents plutôt que les mettre à la corbeille à papier.

De manière similaire, il est souhaitable de mettre en place des procédures claires de destruction ou de recyclage des supports informatiques en fin de vie.

XI - ORGANISER LA RÉACTION EN CAS D'INCIDENT

Lors de la découverte de la compromission d'un équipement (ordinateur infecté par un virus par exemple), il est nécessaire de déterminer rapidement, mais sans précipitation, la démarche qui permettra de juger de la gravité potentielle de l'incident afin de prendre les mesures techniques, organisationnelles et juridiques proportionnées, d'endiguer l'infection et d'isoler les machines compromises. Il est important de réfléchir avant d'agir de manière à ne pas prendre dans l'urgence des décisions qui pourraient s'avérer néfastes.

Disposer d'un plan de reprise et de continuité d'activité informatique, même sommaire, tenu régulièrement à jour décrivant comment sauvegarder les données essentielles de l'entreprise.

Disposer d'un plan de reprise et de continuité d'activité informatique, comprenant idéalement un volet dédié à la réaction en cas d'attaque informatique, est primordial pour une entreprise.

L'analyse des conséquences sur l'activité d'un certain nombre d'événements catastrophiques peut être un bon point de départ : que se passe-t-il si l'accès à Internet ne fonctionne plus pendant deux jours ? Que se passe-t-il si un attaquant efface toutes les données stockées sur les serveurs ?

Les données sensibles de l'entreprise doivent être sauvegardées périodiquement. Cette sauvegarde est de préférence automatique sur les serveurs de fichiers et ne repose pas uniquement sur la bonne volonté des utilisateurs qui risquent fréquemment de ne pas prendre le temps d'effectuer de telles sauvegardes. Les sauvegardes doivent être vérifiées périodiquement et idéalement stockées dans un lieu distinct de celui où se trouvent les serveurs en fonctionnement.

Règle 37

Mettre en place une chaîne d'alerte et de réaction connue de tous les intervenants.

Tous les utilisateurs doivent au minimum pouvoir s'adresser rapidement à un interlocuteur référent, formé à la réaction, pour signaler tout incident. Ils doivent pouvoir joindre cet interlocuteur facilement et doivent être informés qu'il n'est pas souhaitable qu'ils tentent de régler le problème par eux-mêmes.

Lorsque la taille de l'entreprise le permet et dès lors que les enjeux le justifient, il est souhaitable que la chaîne d'alerte comporte un mécanisme d'astreinte voire de permanence permettant de garantir que les incidents constatés puissent être traités le plus efficacement possible.

Règle 38

Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir comment le code malveillant a pu s'installer sur la machine, s'il a pu se propager ailleurs dans le réseau et quelles informations ont été manipulées.

De nombreuses entreprises, en ne cherchant pas d'emblée à connaître le périmètre réel d'une infection, ont perdu plusieurs semaines, voire plusieurs mois, dans le traitement d'un incident. Chaque traitement d'incident doit de plus faire l'objet d'un retour d'expérience et d'une capitalisation permettant d'être plus efficace lorsqu'un événement similaire surgira à l'avenir.

Les questions à se poser sont par exemple les suivantes :

- quelle est la nature du poste compromis ? Y en a-t-il d'autres du même type, exposés aux mêmes menaces sur le réseau ?
- quelles sont les informations auxquelles l'attaquant est susceptible d'avoir eu accès ?
- le poste compromis a-t-il communiqué avec d'autres postes ou serveurs ?

En cas de compromission, et afin de faciliter le travail des équipes d'investigations, les entités responsables pourront prendre les mesures suivantes :

- isoler les machines infectées du réseau (débrancher le câble réseau) ;
- ne pas éteindre électriquement les machines infectées pour préserver les informations disponibles en mémoire sur le code malveillant ;
- réaliser, ou faire réaliser par des spécialistes, des copies des mémoires et des disques durs des machines infectées pour conduire les investigations. Vérifier la bonne intégrité des copies réalisées avant toute opération de mise à jour, de modification de la configuration, de tentative de nettoyage ou de réinstallation des machines compromises ;
- réinstaller intégralement la machine après copie des disques si elle doit être remise en production. Ne jamais se contenter d'une simple restauration ou d'un «nettoyage» que peu d'experts seraient en mesure de pratiquer.

XII - SENSIBILISER

Règle 39

Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires.

Chaque utilisateur devrait en permanence (au minimum chaque année) se voir rappeler :

- que les informations traitées doivent être considérées comme sensibles ;
- que la sécurité de ces informations repose, entre autres, sur l'exemplarité de leur comportement et le respect des règles élémentaires d'hygiène informatique (non-contournement de la politique de sécurité, verrouillage systématique de la session lorsque l'utilisateur quitte sa position informatique, non-connexion d'équipements personnels au réseau de l'entreprise, non-divulgation de mots de passe à un tiers, non réutilisation de mots de passe professionnels dans la sphère privée, signalement des événements suspects, accompagnement des visiteurs et des intervenants extérieurs, etc.).

Le respect des règles d'hygiène qui concernent les utilisateurs devraient figurer dans une charte d'usage des moyens informatiques visée par chaque utilisateur.

XIII - FAIRE AUDITER LA SÉCURITÉ

Règle 40

Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action dont la mise en œuvre est suivie au plus haut niveau.

La réalisation d'audits techniques sur un système d'information est essentielle. En effet, l'audit est le seul moyen efficace de constater concrètement l'efficacité des mesures mises en œuvre sur le terrain. Chaque audit permettra de définir un plan d'actions correctives à mettre en œuvre. Des réunions de suivi de ce plan d'action doivent être organisées fréquemment. Pour une plus grande efficacité, l'avancement du plan d'action devra être synthétisé dans un indicateur du tableau de bord à destination des plus hauts degrés de management.

À propos de l'ANSSI

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a été créée le 7 juillet 2009 sous la forme d'un service à compétence nationale.

En vertu du décret n° 2009-834 du 7 juillet 2009 modifié par le décret n° 2011-170 du 11 février 2011, l'agence assure la mission d'autorité nationale en matière de défense et de sécurité des systèmes d'information. Elle est rattachée au Secrétaire général de la défense et de la sécurité nationale, sous l'autorité du Premier ministre.

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

Version 1.0 - Janvier 2013
20130208-1447

Agence nationale de la sécurité des systèmes d'information

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP
Sites internet : www.ssi.gouv.fr et www.securite-informatique.gouv.fr
Messagerie : communication [at] ssi.gouv.fr