Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

L’hygiène informatique en entreprise

Quelques recommandations simples

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

V0.1 – Octobre 2012

Avant-propos à destination des décideurs

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

Mais protéger ses données et son réseau informatique est crucial pour la survie de l'entreprise et sa compétitivité. Les conséquences qu'auraient pour elle la perte ou le vol de certaines informations ou l'indisponibilité de son informatique 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, etc. A l'inverse, bien protéger les informations confidentielles confiées par des clients et des partenaires peut créer un avantage concurrentiel.

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 joints à des courriels ou dans des clés USB piégés, vol de mots de passe, etc.
Les communications de l'équipe dirigeantes sont souvent une cible privilégiée.

Il est de la responsabilité des dirigeants de vérifier que les mesures de protection adaptées de toutes natures soient 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 appuyée par la direction et périodiquement vérifiée.

Parmi ces mesures, il existe des mesures techniques simples, qualifiées d'hygiène informatique.

De nombreuses attaques informatiques, sur lesquelles l'ANSSI est intervenue, auraient pu être évitées si les mesures essentielles 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 personne qui remplit cette fonction, ce document présente les quelques règles d'hygiène informatique incontournables.

Elles ne prétendent pas avoir un caractère d'exhaustivité. Elles représentent 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 en danger.

Introduction 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.

Base de données des clients, des contrats commerciaux ou des 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 son poste de travail ou son téléphone mobile.

Les conséquences qu'auraient pour votre organisation la perte ou le vol de certaines informations ou l'indisponibilité de son informatique peuvent être lourdes : perte de confiance des clients, des partenaires, des usagers, avantage pris par un concurrent, perte d'exploitation suite à une interruption de la production, vol de données personnelles, etc.

A l'inverse, bien protéger les informations confidentielles confiées par des clients, des partenaires ou des usagers génère la confiance et peut représenter un avantage concurrentiel.

Si les erreurs humaines ou la malveillance d'un employé 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, etc.

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 sont si évidentes et relativement simples à mettre en œuvre, que l'on peut les qualifier de « *règles élémentaires d'hygiène informatique* ». Ne pas les suivre expose 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 quelques règles d'hygiène informatique essentielles pour assurer la sécurité minimale 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 de continuer à servir ses clients ou ses usagers, en respectant l'intégrité et la confidentialité des informations qui les concernent.

Sommaire

Introduction

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

Mais protéger ses données et son réseau informatique est crucial pour la survie de l'entreprise et sa compétitivité. Les conséquences qu'auraient pour elle la perte ou le vol de certaines informations ou l'indisponibilité de son informatique 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, etc. A l'inverse, bien protéger les informations confidentielles confiées par des clients et des partenaires peut créer un avantage concurrentiel.

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, etc.
Les communications de l'équipe dirigeantes sont souvent une cible privilégiée.

Il est de la responsabilité des dirigeants de vérifier que les mesures de protection adaptées de toutes natures 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 appuyée par la direction et périodiquement vérifiée.

Parmi ces mesures, il existe des mesures techniques simples, qualifiées d'hygiène informatique.

De nombreuses attaques informatiques, sur lesquelles l'ANSSI est intervenue, auraient pu être évitées si les mesures essentielles 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 personne qui remplit cette fonction, ce document présente les quelques règles d'hygiène informatique incontournables.

Elles ne prétendent pas avoir un caractère d'exhaustivité. Elles représentent 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 en danger.

I- Connaître précisément 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 oublié des inventaires, cet équipement, qui deviendra rapidement obsolète, sera une cible de choix pour un éventuel attaquant.

Règle 1 - Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour :

Cette cartographie doit au minimum comprendre les éléments suivants :

- liste des briques matérielles et logicielles utilisées ;
- architecture réseau sur laquelle sont identifiés les points névralgiques (connexions externes[1], serveur hébergeant des données et/ou des fonctions sensibles, etc.).

Cette cartographie ne doit 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 sur le système d'information ;
- des utilisateurs qui disposent de privilèges suffisants pour lire la messagerie des dirigeants de la société ou *a fortiori* de l'ensemble des utilisateurs ;
- 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.

Sur un système Windows, la plupart de ces informations peuvent être obtenues par l'analyse de la configuration de l'*Active Directory*. L'article *Audit des permissions en environnement Active Directory*[2] précise un ensemble de méthodes permettant d'en réaliser l'inventaire.

Règle 3 - Rédiger des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires…).

Elles doivent décrire *a minima* :

- la gestion (création / destruction) des comptes informatiques et l'attribution des droits associés à ses comptes sur le système d'information, y compris pour les partenaires et les prestataires externes ;
- la gestion du contrôle d'accès aux locaux ;
- la gestion des équipements mobiles ;
- la gestion du contrôle des habilitations.

---

1 Inventorier en particulier tous les accès Internet du système d'information et 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.

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

II- Maîtriser le réseau

Règle 4 - Limiter le nombre d'accès Internet au strict nécessaire.

Il convient de connaître précisément et de limiter le nombre d'accès Internet et les interconnexions avec des réseaux partenaires au strict nécessaire de manière à pouvoir plus facilement centraliser et homogénéiser la surveillance des échanges.

Règle 5 - Interdire la connexion d'équipements personnels au système d'information de l'entreprise.

Si le travail à distance est nécessaire, l'organisme doit fournir des moyens professionnels pour permettre de tels usages.

III - Mettre à niveau les logiciels

Chaque jour, des vulnérabilités sont mises en évidence dans de très nombreux logiciels largement utilisés. En règle générale, quelques heures seulement sont 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 la maintenance est assurée, d'éviter les technologies trop innovantes ou non maîtrisées en interne et de respecter les recommandations suivantes.

Règle 6 - Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés.

Commencez par 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 compléter l'inventaire avec l'ensemble des autres composants logiciels. Intégrez ces éléments à la cartographie.

Règle 7 - Se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.

Inventoriez les sources susceptibles de remonter des vulnérabilités sur les composants identifiés et de diffuser des mises à jour (site des éditeurs des logiciels considérés, site des CERT).

Règle 8 - 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.

IV- Authentification et mots de passe

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

Règle 9 - Identifier nominativement chaque personne ayant accès au système.

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

Règle 10 - 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 la note de l'ANSSI, *Recommandations de sécurité relatives aux mots de passe*[3].

Règle 11 - Mettre en place des moyens techniques permettant de faire respecter les règles relatives aux mots de passe.

Les moyens permettant de faire respecter la politique 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 ;
- la vérification que les mots de passe choisis ne sont pas trop faciles à retrouver ;
- la vérification que les anciens mots de passe ne facilitent pas la découverte des nouveaux.

Règle 12 - Ne pas conserver les mots de passe sur les systèmes informatiques.

Les mots de passe ou les éléments secrets stockés sur les machines des utilisateurs sont des éléments recherchés ou exploités en priorité par les attaquants.

Règle 13 - Supprimer ou modifier systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).

Les éléments par défaut sont bien souvent 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.).

Règle 14 - Privilégier lorsque c'est possible une authentification forte par carte à puce.

L'ANSSI recommande fortement la mise en œuvre d'une authentification forte reposant sur l'emploi d'une carte à puce dont l'utilisation est assujettie à la connaissance d'un code PIN (voir annexe B.3 du référentiel général de sécurité). La mise en place d'un mécanisme de contrôle d'accès par carte à puce sur un système n'en disposant pas, bien qu'étant une mesure d'hygiène informatique, est cependant plus longue et coûteuse que la mise en œuvre des autres règles décrites dans ce document.

---

[3] Voir sur le site Internet de l'ANSSI : www.ssi.gouv.fr/mots-de-passe

V- Sécuriser les équipements terminaux

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

Règle 15 - Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique, désactiver les services inutiles et restreindre les privilèges des utilisateurs.

Il est en particulier impératif, au minimum, de désactiver les services inutiles et de restreindre les privilèges des utilisateurs.

Règle 16 - Interdire techniquement la connexion des supports amovibles sauf si c'est strictement nécessaire ; sinon 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.

Règle 17 - Utiliser un outil de gestion de parc informatique permettant de déployer des politiques de sécurité et les mises à jour sur les équipements.

Inclure un maximum d'équipements informatiques dans le périmètre des équipements gérés par l'outil en question.

Règle 18 - Gérer les terminaux nomades selon la même politique de sécurité que les postes fixes

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

Règle 19 - Interdire dans tous les cas où cela est possible les connexions à distance sur les postes clients.

Respecter strictement dans le cas contraire les principes décrits dans la note technique Recommandations de sécurité relatives à la téléassistance[4].

Règle 20 – Chiffrer les données sensibles, en particulier sur les postes nomades et les supports perdables.

La perte ou le vol d'équipements (ou de supports) mobiles ou nomades 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 clients) seront en effet compromises, et ce même si le terminal est éteint ou que la session utilisateur est fermée. Il est donc important de chiffrer les données sensibles sur de tels équipements. Plusieurs

[4] Voir sur le site Internet de l'ANSSI : www.ssi.gouv.fr/teleassistance.

produits de chiffrement de disque ou de fichiers (ou supports chiffrants) ont été qualifiés par l’ANSSI. Il convient de les utiliser en priorité.

VI- Segmenter le réseau et contrôler l’annuaire

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 des éléments centraux qui constituent une cible de choix pour les attaquants.

Règle 21 - Auditer ou faire auditer fréquemment la configuration de l'annuaire central (Active Directory en environnement Windows)

On trouvera des conseils dans l’article *Audit des permissions en environnement Active Directory*[5]. Notamment vérifier régulièrement les accès aux données des personnes clés de l’entreprise.

Règle 22 - Ne pas mettre en place de réseaux non 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 »[6], la compromission d'un contrôleur de domaine entraîne systématiquement la compromission de l'ensemble du réseau.

---

5 Voir sur le site Internet de l’ANSSI : www.ssi.gouv.fr/Active-Directory

6 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.

VII- Protéger le réseau interne de l'Internet

Si certaines attaques peuvent avoir une origine interne, l'un des moyens principaux d'infection constatés par l'ANSSI est l'infection suite à la connexion sur un site Internet compromis. En conséquence, l'application des règles relatives à la séparation de la navigation sur Internet et de l'administration s'avère impérative.

Règle 23 - Interdire la navigation sur Internet depuis les comptes d'administration.

Cette interdiction s'applique en particulier aux machines des administrateurs légitimes du système.

Règle 24 - Limiter le nombre de passerelles d'interconnexion avec Internet.

Il faut pour cela mettre en place des services de sécurité correctement configurés (par exemple, conformes à la note Définition d'une architecture de passerelle d'interconnexion sécurisée[7].

Règle 25 - Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis l'Internet.

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

Règle 26 - Éviter l'usage de technologies 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 n'est pas conseillé (faibles garanties en matière de disponibilité, difficultés 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 faire au travers d'une passerelle maîtrisée permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires.
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 accédant au réseau par certificats clients. 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.

---

7 Voir sur le site Internet de l'ANSSI : www.ssi.gouv.fr/architecture-interconnexion

VIII - Surveiller les systèmes

L'ensemble des mesures décrites ci-dessus est des mesures préventives 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 principes suivants.

Règle 27 - Définir concrètement les objectifs de la supervision des systèmes et des réseaux.

Quels sont les événements que l'on souhaite détecter ? Dans la majeure partie des cas, les événements suivants doivent impérativement générer une alerte qui doit impérativement être traitée dans les 24 heures :

- connexion d'un utilisateur hors de ses horaires habituels de travail ;
- transfert massif de données vers l'extérieur de l'entreprise ;
- tentatives de connexions successives ou répétées sur un service.

Règle 28- Déterminer les mécanismes de journalisation devant être activés.

Définir également les procédures de vérification de ces journaux qui permettront de générer une alerte dès lors que l'un des objectifs prioritaires n'est pas rempli.

IX Sécuriser les postes des administrateurs

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

Règle 29 - Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.

Le cloisonnement logique doit idéalement reposer sur un tunnel IPsec mis en œuvre par un produit qualifié par l'ANSSI.

Règle 30 - Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception.

Ne surtout pas faire d'exception pour les dirigeants de l'entreprise.

Règle 31 - N'autoriser l'accès à distance au réseau professionnel, y compris pour l'administration, que depuis des postes professionnels mettant 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 moyens robustes qualifiés par l'ANSSI.

X- Contrôler l'accès aux locaux et 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 sein du réseau interne de l'entreprise, les mesures de sécurité périmétriques mises en place deviennent inefficaces.

Règle 32 - Utiliser impérativement des mécanismes de contrôle d'accès robustes.

Ils doivent permettre de définir des profils d'utilisateurs (employé, prestataire, stagiaire, etc.)

Règle 33 - Gérer 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 ;
- ne jamais donner de clé ou de code d'alarme à des prestataires extérieurs (agents de ménage etc.), sauf s'il est possible de tracer ces accès et de les restreindre techniquement à des plages données.

Règle 34 - Ne pas laisser de prises d'accès au réseau interne accessibles dans les endroits publics.

Ces endroits publics peuvent être des salles d'attente, des couloirs… 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 ;
- écran d'affichage diffusant des flux d'information ;
- prise réseau dans une salle d'attente…

Règle 35 - Définir des règles en matière de gestion des impressions papier.

Les règles suivantes peuvent être définies.

- détruire en fin de journée les documents oubliés sur l'imprimante ou la photocopieuse ;
- broyer les documents plutôt que de 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 qualifier la gravité potentielle de l'incident afin d'y opposer les mesures techniques, organisationnelles et juridiques proportionnées, d'endiguer l'infection et de nettoyer 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.

Règle 36 - Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir si le code malveillant a pu se propager ailleurs dans le réseau.

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 de l'incident.

Règle 37 - Disposer d'un plan de reprise ou de continuité d'activité informatique tenu régulièrement à jour.

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 ?

Règle 38 - Mettre en place une chaîne d'alerte connue de tous les intervenants.

Tous les utilisateurs doivent pouvoir s'adresser à un interlocuteur unique pour signaler tout incident et être incités à le faire.

XII Sensibiliser

Règle 39 - Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires

Chaque utilisateur devrait au minimum chaque année se voir rappeler :

- le fait que les informations traitées doivent être considérées comme sensibles ;
- le fait 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 d'authentifiant à un tiers, signalement des événements suspects).

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.

Des réunions de suivi de ce plan d'action sont organisées fréquemment.

Pour en savoir plus :
recommandations techniques de l'ANSSI : www.ssi.gouv.fr/bonnes-pratiques ;
produits recommandés par l'ANSSI : www.ssi.gouv.fr/certification
www.ssi.gouv.fr/cspn
www.ssi.gouv.fr/qualification

Annexe A : les règles d'hygiène informatique pour les entreprises

1) Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour.
2) Disposer d'un inventaire exhaustif des comptes privilégiés et le maintenir à jour.
3) Rédiger des procédures d'arrivée et de départ des utilisateurs (personnel, stagiaires, …).
4) Limiter le nombre d'accès Internet au strict nécessaire.
5) Interdire la connexion d'équipements personnels au système d'information de l'entreprise.
6) Connaître les modalités de mises à jour de l'ensemble des composants logiciels utilisés.
7) Se tenir informé des vulnérabilités de ces composants et des mises à jour nécessaires.
8) Définir une politique simple de mise à jour et l'appliquer strictement.
9) Identifier nominativement chaque personne ayant accès au système.
10) définir des règles de choix et de dimensionnement des mots de passe
11) Mettre en place des moyens techniques permettant de faire respecter les règles relatives aux mots de passe.
12) Ne pas conserver les mots de passe sur les systèmes informatiques.
13) Supprimer ou modifier systématiquement les éléments d'authentification par défaut (mots de passe, certificats) sur les équipements (commutateurs réseau, routeurs, serveurs, imprimantes).
14) Privilégier lorsque c'est possible une authentification forte par carte à puce.
15) Mettre en place un niveau de sécurité homogène sur l'ensemble du parc informatique, désactiver les services inutiles et restreindre les privilèges des utilisateurs.
16) Interdire techniquement la connexion des supports amovibles sauf si c'est strictement nécessaire ; sinon désactiver l'exécution des *autoruns* depuis de tels supports.
17) Utiliser un outil de gestion de parc informatique permettant de déployer des politiques de sécurité et les mises à jour sur les équipements.
18) Gérer les terminaux nomades selon la même politique de sécurité que les postes fixes
19) Interdire dans tous les cas où cela est possible les connexions à distance sur les postes clients.
20) Chiffrer les données sensibles, en particulier sur les postes nomades et les supports perdables.
21) Auditer ou faire auditer fréquemment la configuration de l'annuaire central (Active Directory en environnement Windows)
22) Ne pas mettre en place de réseaux non cloisonnés. Pour les postes ou les serveurs contenant des informations importantes pour la vie de l'entreprise, créer un sous-réseau protégé par un pare-feu spécifique.
23) Interdire la navigation sur Internet depuis les comptes d'administration.
24) Limiter le nombre de passerelles d'interconnexion avec Internet.
25) Vérifier qu'aucun équipement du réseau ne comporte d'interface d'administration accessible depuis l'Internet.
26) Éviter l'usage de technologies 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.
27) Définir concrètement les objectifs de la supervision des systèmes et des réseaux.
28) Déterminer les mécanismes de journalisation devant être activés.
29) Utiliser un réseau dédié à l'administration des équipements ou au moins un réseau logiquement séparé du réseau des utilisateurs.
30) Ne pas donner aux utilisateurs de privilèges d'administration. Ne faire aucune exception.
31) N'autoriser l'accès à distance au réseau professionnel, y compris pour l'administration, que depuis des postes professionnels mettant en œuvre des mécanismes

d'authentification forte et protégeant l'intégrité et la confidentialité des échanges à l'aide de moyens robustes (privilégier ceux qui sont qualifiés par l'ANSSI).

32) Utiliser impérativement des mécanismes de contrôle d'accès robustes.
33) Gérer rigoureusement les clés permettant l'accès aux locaux et les codes d'alarme.
34) Ne pas laisser de prises d'accès au réseau interne accessibles dans les endroits publics.
35) Définir des règles en matière de gestion des impressions papier.
36) Ne jamais se contenter de traiter l'infection d'une machine sans tenter de savoir si le code malveillant a pu se propager ailleurs dans le réseau.
37) Disposer d'un plan de reprise ou de continuité d'activité informatique tenu régulièrement à jour.
38) Mettre en place une chaîne d'alerte connue de tous les intervenants.
39) Sensibiliser les utilisateurs aux règles d'hygiène informatique élémentaires.
40) Faire réaliser des audits de sécurité périodiques (au minimum tous les ans). Chaque audit doit être associé à un plan d'action.

Annexe B : Pour en savoir plus

Sur le site Internet de l'ANSSI :

- recommandations techniques de l'ANSSI : www.ssi.gouv.fr/bonnes-pratiques ;
- produits recommandés par l'ANSSI : www.ssi.gouv.fr.

Guides généraux pour les entreprises :

- guide SSI du MEDEF – mai 2005 – disponible sur Internet (sites de la CCIP et de l'Union Patronale du Var.
- Guide pratique à l'usage des dirigeants – 2010 - région Rhône-Alpes – téléchargeable sur le site de l'Espace Numérique Entreprises : www.ene.fr/actualites/information-pme/secu