MINISTÈRE
DE LA JUSTICE
Liberté
Égalité
Fraternité

DIRECTION DE L'ADMINISTRATION PÉNITENTIAIRE

****

CONCOURS EXTERNE ET INTERNE POUR LE RECRUTEMENT DE TECHNICIENS DE L'ADMINISTRATION PÉNITENTIAIRE

SESSION 2024

SPÉCIALITÉS LIÉES À L'INFORMATIQUE

Une épreuve écrite d'admissibilité commune aux deux concours qui consiste en l'étude de cas ou d'un dossier technique permettant d'apprécier les qualités de réflexion et le sens de l'organisation du candidat.

(durée de l'épreuve : 3 heures ; coefficient : 4)

****

Cette épreuve comporte l'analyse d'une situation nécessitant un traitement ou une opération technique ainsi que la rédaction d'un compte rendu ou d'un rapport d'intervention présentant les solutions adaptées au cas soumis (telles que gestion prévisionnelle de travaux, organisation d'une production ou d'un chantier).

Cette épreuve peut faire appel à des notions élémentaires du code des marchés publics, des règles sur la maîtrise d'ouvrage publique et des dispositions relatives à l'hygiène et la sécurité au travail.

Les problèmes posés peuvent se présenter sous la forme de questionnaire à choix multiples, fiches techniques, tableaux, grilles, diagrammes, plans, schémas ou croquis à analyser, à remplir, à compléter ou tout autre mode d'interrogation du même type.

Le sujet noté sur 100 points, comporte 28 pages dont 23 pages d'annexes.

Le candidat ne doit pas répondre sur le sujet. Chaque réponse doit être reportée sur votre copie en rappelant le numéro de la question.

L'usage de documents autres que ceux fournis dans ce sujet, matériel informatique ou smartphone ne sont pas autorisés. Seule la calculatrice non programmable est autorisée.

Tournez la page S.V.P

Annexes

Document 1 - Extrait Guide ANSSI « Recommandation relatives à l'administration sécurisée des systèmes d'information » (10 pages)

Document 2 - Action prioritaire (1 Page)

Document 3 – SMTP (5 pages)

Document 4 - ITIL (2 pages)

Document 5 – Le rançongiciel (2 pages)

Document 6 - RSSI dans la chaine SSI (3 pages)

Tournez la page S.V.P

PREMIÈRE PARTIE (40 points)

QUESTIONS D'ORDRE GÉNÉRAL (10 points)

1.1) En informatique, à quoi sert le modèle OSI ? Citez au moins 4 couches du modèle.

1.2) Que signifie l'acronyme RSSI ? Définir ses missions.

1.3) Dans les projets informatiques, qu'évoquent pour vous les termes MOA et MOE ?

1.4) Combien de canaux peut-on souscrire au maximum avec un abonnement T2 ?

1.5) Quelle est la différence entre une ligne ADSL et une ligne Fibre Optique ?

QUESTIONS D'ORDRE TECHNIQUE (30 points)

1.6) Quel est la différence entre LAN et WAN ?

1.7) Quelle est la différence entre un routeur et un commutateur réseau ?

1.8) Quelle est la différence entre une adresse MAC et une adresse IP ?

1.9) Quel est le rôle d'un « Pare-feu » ?

1.10) Que signifie l'acronyme SSD pour les disques durs ?

1.11) Expliquez son fonctionnement.

1.12) Qu'est-ce qu'un rançongiciel ?

1.13) Quel type de périphérique permet une installation HotPlug ?

- PCI
- Série
- USB

1.14) Quel protocole utilise le port 25 ? Définissez-le.

1.15) Quelles normes sont utilisés dans les réseaux WiFi ?

1.16) Expliquez la fonction d'un serveur « DNS » ?

1.17) Qu'est-ce que le service SMB ?

1.18) Que signifie l'acronyme « Nslookup » ?

1.19) A quoi sert cette commande ?

1.20) Qu'est-ce qu'un SPAM ?

1.21) Définissez ce qu'est un VPN ? Expliquez son mode de fonctionnement et citez un cas d'utilisation.

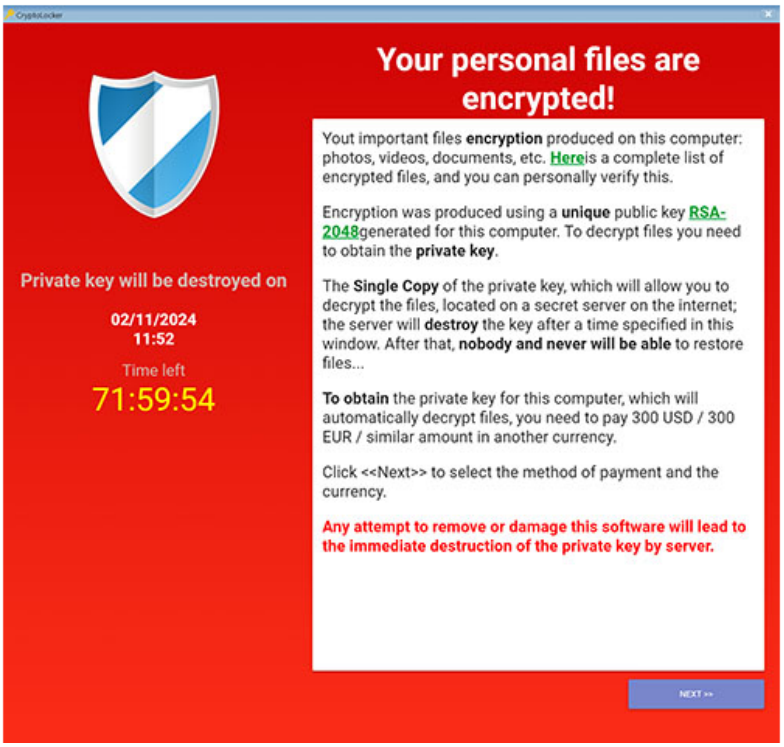
DEUXIEME PARTIE (60 points)

ETUDE DE CAS

Cas n°1 : (35 points)

En tant que correspondant local des systèmes d'information au sein d'un établissement pénitentiaire vous êtes en charge du bon fonctionnement du système d'information et de la sécurité de celui-ci.

Un agent vous appelle car en connectant sa clef USB professionnelle sur son poste informatique relié au réseau du site, un message est apparu (ci-dessous) et l'empêche de poursuivre son activité correctement.



1. Quelles sont les étapes que vous mettez en œuvre afin de contenir l'infection et remettre en fonction le poste de l'agent ?
2. Dans vos démarches de traitement de résolution de l'incident, qui sont les interlocuteurs que vous allez solliciter ?

Le chef d'établissement vous demande de rédiger :

- Une note d'information à destination de l'ensemble du personnel de l'établissement afin de rappeler les bonnes pratiques sur l'usage d'un dispositif de stockage amovible. (*Faites une proposition en 20 lignes maximum*).

- Un rapport d'écrivant votre plan d'action ainsi que les procédures que vous pourriez mettre en place afin d'avoir une traçabilité des stockages amovibles au sein de l'établissement et responsabiliser les utilisateurs.

Cas n°2 : (25 points)

Vous êtes responsable de l'unité technique au sein de la Direction interrégionale des services pénitentiaires de Dijon, votre responsable vous demande de travailler sur un nouvel établissement reparti sur 3 sites distants de plus de 10km des uns des autres.

Vous trouverez ci-dessous le détail des équipements sur chacun de ces sites :

- Site n°1 : 250 postes de travail, 10 copieurs, 5 serveurs de bureautique, 1 serveur de messagerie, accès internet ;
- Site n°2 : 50 postes de travail, 1 serveur de bureautique, 2 copieurs, accès internet ;
- Site n°3 : 10 postes de travail, 1 serveur de bureautique, 1 copieur, accès internet.

Dans vos réponses, vous prendrez en compte que la sécurité informatique est au cœur des préoccupations du Directeur et doit être conforme aux bonnes pratiques de la sécurité informatique.

Question 1 : (15 Points)

a) Proposez les différents moyens pour interconnecter ces différents sites.

b) Sur le site n°1, lister deux équipements réseau que vous allez utiliser.

c) Faire un schéma de l'architecture physique de votre réseau.

Question 2 : (5 points)

Les stations de travail sont dorénavant équipées de téléphones IP.

Citez 4 impacts sur votre infrastructure réseau.

Question 3 : (5 points)

Le technicien d'astreinte doit pouvoir intervenir rapidement de chez lui en cas de problème informatique via l'internet. Quelle solution réseau permet de répondre à cette problématique ?

RECOMMANDATIONS RELATIVES À L'ADMINISTRATION SÉCURISÉE DES SYSTÈMES D'INFORMATION

GUIDE ANSSI

ANSSI-PA-022
11/05/2021

PUBLIC VISÉ :

Développeur | **Administrateur** | **RSSI** | **DSI** | Utilisateur

Tournez la page S.V.P

1
Introduction

1.1 Objectif du guide

L'administration d'un SI se traduit par un ensemble de mesures techniques et non techniques visant entre autres à maintenir le SI en condition opérationnelle et de sécurité et à gérer des changements mineurs ou des évolutions majeures.

Ce guide décrit les objectifs de sécurité et les principes d'élaboration d'une architecture technique sécurisée d'administration. Il propose des éléments utiles d'aide à la conception. Il présente quelques cas d'usages concrets mais n'a pas vocation à être exhaustif.

Ce document s'adresse à des lecteurs qui disposent de connaissances minimales pour appréhender les recommandations de sécurité présentées, capables de les adapter à leur contexte et à leurs besoins. Chacun doit s'appuyer également sur la politique de sécurité du système d'information de son entité et sur les résultats d'une analyse de risque pour déterminer les recommandations les plus pertinentes à mettre en œuvre.

1.2 Organisation du guide

Ce guide tente d'aborder l'ensemble des thèmes liés à l'administration d'un SI et liste des recommandations dont l'implémentation peut être plus ou moins complexe suivant le contexte de l'entité. L'application linéaire de ce guide ne saurait être adaptée à tous les contextes.

Après une première lecture pour s'approprier les concepts, il est recommandé d'évaluer le niveau de maturité de l'entité sur le sujet de l'administration d'un SI à l'aide de la liste des recommandations (p. 63). Pour chaque recommandation, préciser si elle est « *respectée* », « *partiellement respectée* » ou « *non respectée* ». Une fois synthétisée, cette analyse peut être le point de départ d'un plan d'actions visant le respect le plus exhaustif possible des recommandations du guide tout en gardant un esprit critique vis-à-vis du contexte d'application.

1.3 Convention de lecture

Pour chacune des recommandations de ce guide, l'utilisation du verbe *devoir* est volontairement plus prescriptive que la formulation *il est recommandé*.

Pour certaines recommandations de ce guide, il est proposé, au vu des menaces constatées lors de la rédaction de ce guide, plusieurs solutions qui se distinguent par le niveau de sécurité qu'elles

permettent d'atteindre. Le lecteur a ainsi la possibilité de choisir une solution offrant la meilleure protection en fonction du contexte et de ses objectifs de sécurité.

Ainsi, les recommandations sont présentées de la manière suivante :

R

Recommandation à l'état de l'art

Cette recommandation permet de mettre en œuvre un niveau de sécurité à l'état de l'art.

R -

Recommandation alternative de premier niveau

Cette recommandation permet de mettre en œuvre une première alternative, d'un niveau de sécurité moindre que la recommandation R.

R --

Recommandation alternative de second niveau

Cette recommandation permet de mettre en œuvre une seconde alternative, d'un niveau de sécurité moindre que les recommandations R et R -.

R +

Recommandation renforcée complémentaire

Cette recommandation complémentaire permet de mettre en œuvre un niveau de sécurité renforcé. Elle est destinée en priorité aux entités qui sont matures en sécurité des systèmes d'information.

La liste récapitulative des recommandations est disponible en page 63.

Tournez la page S.V.P

2
Les administrateurs, acteurs clés de la sécurité du système d'information

Ce chapitre introductif, consacré au rôle d'administrateur, vise à présenter l'ensemble du lexique relatif à l'administration du SI et sert donc de référence pour l'ensemble du document. Il est également un résumé des différentes thématiques abordées.

2.1 Les administrateurs dans l'écosystème du SI de l'entité

Un administrateur est non seulement un acteur essentiel du système d'information mais aussi un contributeur majeur pour sa sécurité. Il peut être un salarié de l'entité (on parle d'*administrateur interne*) ou un sous-traitant de l'entité (on parle d'*administrateur externe*), indépendamment du lieu d'activité. De plus, qu'il soit administrateur technique (réseau, système) ou administrateur métier, les besoins d'accès et de privilèges ne sont généralement pas uniformes ; les administrateurs peuvent être regroupés par catégories.

Un administrateur est une ressource critique investie de capacités techniques d'accès aux informations métier de l'entité. En effet, il se distingue des autres utilisateurs par les privilèges qui lui sont accordés sur le système d'information. Il dispose de *droits d'administration* nécessaires à la bonne réalisation d'*actions d'administration*.

Actions d'administration

Ensemble des actions d'installation, de suppression, de modification et de consultation de la configuration d'un système participant au SI et susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.

Il est nécessaire de dissocier clairement les différents rôles d'un administrateur sur le SI : un rôle d'utilisateur standard du SI sans privilèges particuliers et un ou plusieurs rôles d'administrateur. Cela se traduit entre autres par la création d'un compte utilisateur standard pour utiliser le SI hors administration et d'un ou plusieurs *comptes d'administration* dédiés aux actions d'administration. L'identification et l'authentification des administrateurs sont les sujets du chapitre 7.

Un poste utilisé pour les actions d'administration, dénommé *poste d'administration*, est un terminal matériel ; il peut être fixe ou portable suivant les besoins. Il est l'objet du chapitre 4.

Un administrateur réalise ses actions grâces à des *outils d'administration*, généralement logiciels, mis à sa disposition sur un poste d'administration ou sur des serveurs dédiés. Un client SSH, une

console centralisée de gestion d'annuaire, un portail Web d'administration de pare-feu sont des exemples d'outils d'administration. Le chapitre 6 aborde ce sujet.

En cas d'accès distant d'un administrateur (ex. : astreinte à domicile, déplacement), on parle d'*administration à distance* dans le chapitre 10. Le cas particulier de l'administration ou l'assistance à distance par des tiers est abordé dans le chapitre 12.

Partie intégrante du SI de l'entité au sens large, le *système d'information d'administration* est le sujet de ce guide. Il inclut toutes les *ressources d'administration* nécessaires pour administrer le SI considéré dont les *postes d'administration*, les *serveurs d'outils* d'administration et les *infrastructures d'administration* nécessaires à son bon fonctionnement (serveurs d'annuaire, DNS, etc.).

Ces ressources sont connectées sur un *réseau d'administration*, réseau de communication faisant transiter les flux internes au SI d'administration et les *flux d'administration* à destination des *ressources administrées*. Ce réseau est évoqué dans le chapitre 5.

La figure 2.1, à titre d'exemple, est un résumé sous forme de représentation fonctionnelle.

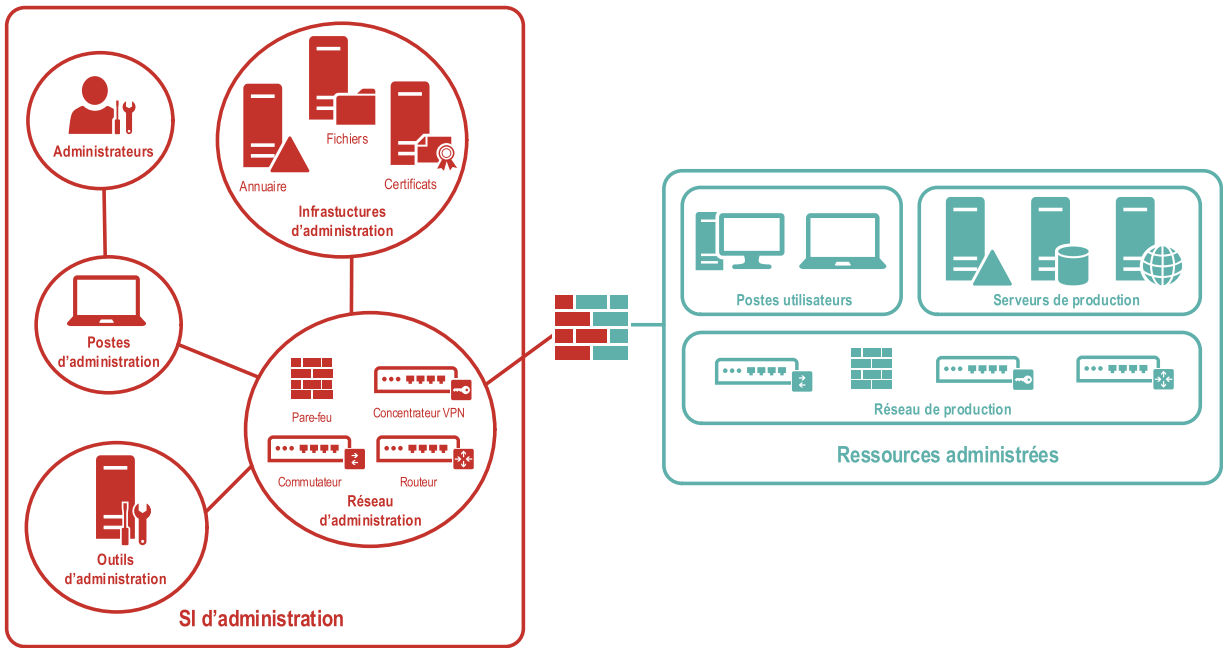


FIGURE 2.1 – Représentation fonctionnelle d'un SI d'administration et de ressources administrées

En périphérie du SI d'administration, un système d'échange sécurisé, illustré par la figure 2.2 et présenté dans le chapitre 11, peut être positionné pour des échanges avec d'autres SI (ex. : un SI bureautique connecté à Internet).

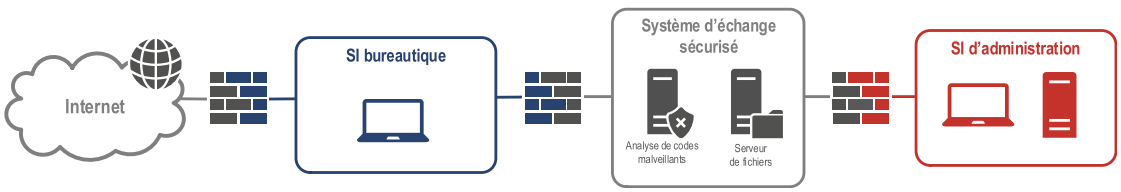


FIGURE 2.2 – Représentation fonctionnelle d'un système d'échange sécurisé

Tournez la page S.V.P

2.2 Droits et devoirs des administrateurs

Les fonctions d'administrateur, complexes, doivent s'équilibrer entre un grand pouvoir impliquant de grandes responsabilités et le respect d'obligations précises. En particulier, un administrateur d'un système d'information est tenu à des obligations de loyauté (respect des règles d'éthique), de transparence (respect du règlement intérieur et de la charte informatique) et de confidentialité [1] (respect du secret professionnel). Le non-respect de ces obligations peut donner lieu à des sanctions disciplinaires (allant jusqu'au licenciement pour faute grave), voire des sanctions pénales. L'annexe B traite plus en détail les aspects juridiques, notamment les différents droits et devoirs des administrateurs.

En premier lieu, les droits et obligations des salariés, dont font partie les administrateurs, pour l'utilisation des moyens informatiques doivent être consignés dans une charte informatique annexée au règlement intérieur ou au contrat de travail. L'entité peut prévoir en complément une charte informatique spécifique applicable aux administrateurs. Cette charte doit notamment appeler les administrateurs à la vigilance vis-à-vis des ressources d'administration mises à leur disposition et sur les conduites à tenir en cas de compromission avérée ou suspectée, de perte ou de vol. Pour toute question relative à la sécurité des systèmes d'information (SSI), un administrateur doit pouvoir s'adresser à des référents internes de l'entité, clairement identifiés, techniques ou non techniques.

R1

Informer les administrateurs de leurs droits et devoirs

Un administrateur doit être informé de ses droits et devoirs, notamment en s'appuyant sur la charte informatique de l'entité.
Il est recommandé d'élaborer une charte informatique spécifique applicable aux administrateurs.

Le rôle d'administrateur nécessite non seulement une confiance forte de l'entité au regard de la criticité de ses actions sur le SI mais également des compétences techniques élevées. Les formations initiale et continue des administrateurs sont indispensables pour garantir la maîtrise de toutes les compétences requises par l'exercice de leurs fonctions.

R2

Former les administrateurs à l'état de l'art en matière de SSI

En tant que ressource humaine critique pour le SI, un administrateur doit être formé à l'état de l'art, dans ses domaines de compétences et en sécurité des systèmes d'information (ex. : sécurité des systèmes, sécurité des réseaux, infrastructure de gestion de clés).
Le guide d'hygiène informatique de l'ANSSI [13] doit être connu.

Quels que soient l'organisation de l'entité et le partage des responsabilités (entre architectes et administrateurs par exemple), il est essentiel de concevoir et de maintenir à jour la documentation des SI : schémas d'architecture, plans d'adressage IP, matrices de flux, inventaire des comptes privilégiés, etc.

1. Se reporter au guide pour les employeurs et les salariés élaboré par la CNIL [1] dont notamment la fiche n°7 pour les administrateurs.

R3

Disposer d'une documentation des SI à jour

Les administrateurs doivent disposer de documents reflétant fidèlement l'état courant des SI qu'ils administrent, notamment des cartographies du SI (physique, système, réseau, applications) faisant notamment apparaître clairement les interconnexions avec l'extérieur.

Tournez la page S.V.P

3
Généralités sur le système d'information d'administration

3.1 Analyse de risque et objectifs de sécurité

Les ressources d'administration sont des cibles privilégiées par un attaquant. En effet, les droits élevés nécessaires à la réalisation des actions d'administration et les larges accès généralement attribués exposent ces ressources à une menace élevée. Dans de nombreux cas de compromission ou d'intrusion sur ces équipements, l'attaquant prend le contrôle de l'ensemble du SI.

3.1.1 Analyse de risque

Ce guide n'a pas vocation à établir une analyse de risque exhaustive ; ce travail essentiel, propre à chaque système d'information, incombe aux entités en ayant la responsabilité, en liaison avec les responsables de la sécurité des systèmes d'information (RSSI). L'analyse de risque peut être menée avec la méthode EBIOS *Risk Manager* [18] par exemple.

Ainsi, les architectures du SI d'administration peuvent varier en fonction de la criticité du SI administré ou des usages par différentes populations d'administrateurs, chacun ne relevant pas du même niveau de confiance, par exemple entre administrateurs internes et externes.

R4

Mener une analyse de risque sur le SI d'administration et son écosystème

Avant toute étude des mesures techniques à mettre en œuvre, une analyse de risque doit être menée en portant une attention particulière sur les besoins de sécurité du SI d'administration et ses interconnexions.
Dans une démarche d'amélioration continue, il est recommandé que l'analyse de risque et la mise en œuvre des mesures induites soient revues au moins une fois par an.

3.1.2 Objectifs de sécurité

Le premier objectif de sécurité des recommandations de ce guide est de protéger le SI d'administration de toute tentative de compromission. En effet, le scénario de compromission le plus fréquent est l'exécution d'un code malveillant sur le poste d'administration – ou sur un poste sur lequel un administrateur s'est connecté avec ses privilèges d'administrateur. Ce code malveillant peut être introduit par le biais d'une navigation Web, par l'ouverture d'une pièce jointe dans un courriel piégé ou à partir d'un support amovible.

Tournez la page S.V.P

Scénario d'attaque

Un code malveillant peut profiter par exemple des privilèges élevés de la session d'un administrateur pour exécuter des actions telles que :

- le vol des empreintes de mots de passe sur le poste, par exemple par une copie mémoire (ex. : attaque *Pass The Hash* qui permet la réutilisation de ces empreintes pour accéder, sans connaître le mot de passe et donc sans devoir le recouvrer, aux ressources du système d'information) ;
- l'installation d'un logiciel espion (ex. : cheval de Troie, enregistreur de frappes clavier – *keylogger*) ;
- l'accès à un serveur de commande et de contrôle [2] ;
- la diffusion d'un ver informatique.

Le deuxième objectif de sécurité est de protéger le SI administré des intrusions et compromissions pour lesquelles le SI d'administration serait un vecteur d'attaque. Dans ce cas, on cherche à minimiser les conséquences sur le SI administré d'une compromission du SI d'administration. Du fait des privilèges élevés du SI d'administration sur le SI administré, une action malveillante reste possible mais un cloisonnement adéquat du SI d'administration doit permettre d'éviter une compromission totale du SI administré.

3.2 Zones de confiance et zones d'administration

Pour réduire la surface d'exposition aux attaques informatiques et les conséquences en cas de compromission, il est nécessaire de procéder à un découpage du SI administré en zones homogènes dites *zones de confiance* puis d'en déduire des *zones d'administration* au sein du SI d'administration.

Zone de confiance

Une zone de confiance comprend exclusivement des ressources homogènes ; elle est administrée par des administrateurs de même niveau de confiance.

Le découpage du SI administré en zones de confiance peut être déterminé par la combinaison de plusieurs critères d'homogénéité, parmi lesquels :

- de criticité métier (ex. : haute, moyenne, basse) ;
- organisationnels (ex. : administration interne ou infogérée) ;
- d'exposition (ex. : à Internet, à des fournisseurs, exclusivement interne) ;
- réglementaires (ex. : données de santé, données personnelles, données relevant du secret de la défense nationale) ;
- géographiques (ex. : découpage par pays).

Par défaut, à une zone de confiance correspond une zone d'administration. Les cas de mutualisation sont évoqués dans la section 13.2.

2. Un serveur de commande et de contrôle (C&C) est un ordinateur qui donne des ordres aux équipements infectés par un logiciel malveillant et qui reçoit des informations de ces équipements.

Ce découpage du SI administré (et les conséquences sur le SI d'administration pour la définition des zones d'administration) doit être mené aussi bien en phase de conception initiale qu'avant toute évolution significative du SI administré. Il permet en effet d'alimenter les travaux d'architecture afin que soit traité dans la continuité l'ensemble des besoins d'administration.

Des mécanismes techniques de cloisonnement sont alors mis en œuvre pour matérialiser les zones d'administration : filtrage, chiffrement, authentification, etc. Ainsi, en respectant le principe du moindre privilège, un administrateur donné n'a accès qu'à la ou les zones d'administration dont il a le juste besoin opérationnel, sans possibilité technique d'accéder à une autre zone.

R5

Définir les zones de confiance du SI administré et déduire les zones d'administration

Avant toute étude d'architecture du SI d'administration, un découpage du SI administré en zones de confiance doit être réalisé. Ce travail permet de déduire un découpage du SI d'administration en zones d'administration.

3.3 Produits qualifiés par l'ANSSI

La qualification [27] prononcée par l'ANSSI permet d'attester d'un certain niveau de sécurité et de confiance dans les produits [3] et les prestataires de service. Ce processus permet de s'assurer notamment que des produits remplissent les objectifs de sécurité définis dans des cibles de sécurité préalablement approuvées.

Il est recommandé de recourir à des produits qualifiés pour la protection du SI d'administration même si l'entité n'est soumis à aucun texte réglementaire. Une attention particulière sera portée sur la cible de sécurité qui précise le périmètre qualifié du produit (ex. : le filtrage dynamique des flux IP aux niveaux 3 et 4 pour un pare-feu) ainsi que les hypothèses d'environnement.

R6

Privilégier l'utilisation de produits qualifiés par l'ANSSI

D'une manière générale, il est recommandé que les matériels et les logiciels utilisés pour protéger le SI d'administration soient qualifiés par l'ANSSI au niveau requis par les besoins de sécurité.
À défaut, il est recommandé qu'ils disposent d'un autre visa de sécurité délivré par l'ANSSI [4].

Attention

Il est recommandé d'être toujours attentif aux versions de matériel ou logiciel auxquelles ils s'appliquent ainsi qu'à la définition de la cible de sécurité.

3. La qualification des produits par l'ANSSI comporte trois niveaux : élémentaire, standard et renforcé.
4. Se reporter à `https://www.ssi.gouv.fr/visa-de-securite`.

Tournez la page S.V.P

Comment classer les actions prioritaires ?

De nombreuses méthodes existent pour vous aider, parmi lesquelles :

Le classement A-B-C-D

Comment faire ? Eclatez votre liste de tâches suivant la classification suivante :

- **A / Les tâches incontournables à mener .** Pour certaines, la question ne se pose pas, tellement les enjeux sont importants. Elles doivent être traitées immédiatement.
- **B / Celles qui sont importantes, mais un cran en-dessous des premières .** Les enjeux sont plus modérés en terme de délai et/ou d'impact.
- **C / Classez ici celles qui sont intéressantes à faire ,** mais qui n'ont pas d'impact. C'est du plus.
- **D / Celles à éliminer : ce sont celles qui n'apportent aucune valeur ajoutée.** C'est le cas de quelques tâches administratives.

Passez en revue chaque catégorie, et à l'intérieur de chacune, refaites un classement : A1 - A2 - A2 - B1... de la plus importante, prioritaire, à la moins urgente. Vous obtenez ainsi votre liste priorisée.

Une petite astuce : si vous hésitez pour une tâche, comparez-là avec d'autres déjà classées : "Laquelle des 2 est la plus importante ?". Vous saurez ainsi où la positionner.

La matrice importance / urgence

Cette matrice repose également sur 4 cases combinant 2 axes : **importance et urgence** . Elle permet de ventiler chaque item suivant ces 2 critères pour aboutir à une lecture synthétique des priorités. Bien évidement, **les tâches de la case "important/urgent" requièrent une action au plus vite .**

Vous pouvez aussi prendre en considération d'autres critères, comme **le temps requis pour executer la tâche**, ou tenir compte de la **facilité de traitement** .

Passez en revue vos actions de la journée et classez-les en utilisant l'une de ces méthodes .

N'oubliez pas enfin de **déléguer ce qui peut l'être** . Vouloir tout faire n'a pas de sens si vous n'avez pas le temps de tout traiter dans les délais impartis.

Tournez la page S.V.P

C’est quoi un serveur SMTP ?

By Master isolated images

En voyant l'image associée à l'article, je vous donne un petit indice pour répondre à la question … Qu'est-ce qu'un serveur SMTP ?

Si vous ne connaissez pas le principe de fonctionnement des mails, je vous conseille de lire : Comment ça marche les mails ?

Définition d’un serveur SMTP

Un serveur SMTP est un serveur qui va permettre l’envoi des mails.

- Mais comment c’est fait ?
- A quoi ça sert ?
- Lequel utiliser ?
- Est-ce que j’ai besoin de connaître ça ?

Eh bien, ça en fait des questions auxquelles je vais essayer de répondre simplement.

Voici ce que vous trouverez sur cet article

- La signification de SMTP
- Le fonctionnement du SMTP
- Les différents modes de connexion possibles au SMTP
- Les principaux serveurs SMTP, POP et IMAP des fournisseurs d’accès.

Signification de SMTP

C’est un procotole (langage) pour envoyer des mails.

SMTP = Simple Mail Transfer Protocol = Protocole Simple pour le Transfert des Mails.

Vous le savez peut-être mais, le mail est :

- un des services qui a contribué au succès d’Internet,
- et un des services plus utilisés sur Internet (saviez-vous qu’au début d’Internet presque 80% des échanges étaient des échanges de mails ?).

On parle toujours de serveur SMTP, mais dans les entreprises, il est rare que le serveur qui supporte le service SMTP ne fasse que ça.

Le fonctionnement du SMTP

Même si pour envoyer un mail, vous n'avez pas besoin de savoir comment fonctionne le SMTP : pour votre culture, voici comment cela se passe.

Pour envoyer un mail, vous utilisez un M.U.A. (Mail User Agent), il est en général de 2 types :

- un webmail (lorsque vous vous connectez en ligne)
- un client de messagerie (logiciel installé sur votre ordinateur tel que Outlook, ThunderBird, application de Smartphone, …)

Au moment ou vous envoyez votre mail, votre MUA :

- va convertir votre mail au format texte (même les pièces jointes seront converties en texte)
- va se connecter au serveur SMTP qui est paramétré et envoyer le texte.

Ensuite, le serveur SMTP va envoyer le mail vers le destinataire. Si le message doit passer entre différents serveurs, c'est toujours le protocole SMTP qui sera utilisé pour envoyer le message de serveurs en serveurs, les serveurs utilisent alors des relais SMTP.

Le mail va ainsi voyager de serveurs en serveurs, jusqu'au dépôt sur le serveur de boites postales du destinataire.

Un petit comparatif avec ce qui se passe lorsque vous envoyez un courrier papier devrait faciliter la compréhension de tout ça.

(en gris, toutes opérations effectuées par le serveur SMTP ou le relai SMTP).

Courrier postal	Mail
Je rédige mon courrier (sur une feuille de papier)	Je rédige mon mail (avec l'aide d'un logiciel ou d'un webmail)
Je mets le courrier dans une enveloppe et j'inscris l'adresse du destinataire.	Je saisis l'adresse mail du destinataire.
Je mets mon adresse au dos de l'enveloppe * *(voir plus bas)*	Je n'ai rien à faire, cela est déjà fait par le logiciel.
Je mets le courrier dans la boite aux lettres de la poste.	Je clique sur envoyer
Lors de la relève de la boite postale, la poste récupère tous les courriers	Mon logiciel s'est connecté au serveur SMTP et le serveur SMTP récupère le mail.
Le courrier est trié et en envoyé vers le bureau de poste du destinataire	Le serveur SMTP va envoyer le mail.
Le courrier va passer de centre de tri en centre de tri.	Le mail va passer de serveurs SMTP en serveurs SMTP (on appelle cela des relais SMTP).
Le courrier arrive au bureau de poste du destinataire et le facteur va le déposer dans la boite aux lettres du destinataire.	Il arrive sur le serveur de l'hébergeur de la boite aux lettres du destinataire.
Le destinataire va avec sa clé ouvrir sa boite aux lettres et ouvrir son courrier.	Avec son logiciel de mail ou son webmail, le destinataire va ouvrir sa boite aux lettres (avec son mot de passe) et lire son mail.

Tournez la page S.V.P

** Le fait de mettre mon adresse au dos va permettre de me renvoyer le courrier en cas d'erreur d'adresse de destination.*

Il n'y a pas de contrôle effectué sur l'expéditeur : vous pouvez bien mettre une autre adresse que la votre au dos de la lettre, et faire croire ici que c'est quelqu'un d'autre qui envoie le courrier : c'était comme ça au début du mail, on pouvait mettre l'adresse de quelqu'un d'autre. Cela est toujours possible sur certains serveurs, et c'est pour cela que sur les autres, il faut s'identifier avant d'envoyer le mail.

Modes de connexion au serveur SMTP.

Pour se connecter au serveur, le logiciel utilise des commandes très simple en mode texte.

Il existe différents modes de connexions au serveurs SMTP.

Le 1er mode de connexion utilisait le port 25 et se faisait sans authentification (sans fournir de login et de mot de passe). Cela était très pratique car il était simple d'envoyer des mails. Tout le monde pouvait se connecter à n'importe quel serveur sans aucune autorisation et il était possible d'envoyer des messages avec n'importe quelle adresse (on pouvait donc usurper l'adresse mail de quelqu'un).

Il a fallut remédier à ça, mais il reste encore des serveurs SMTP sans authentification (on parle de « relais ouverts ») : ils font le bonheur des spammeurs. Certains fournisseurs d'accès refusent les messages provenant de ces relais ouverts.

Pour tous les autres serveurs SMTP, plus sérieux, il faut désormais un compte (login) ou adresse mail, ainsi qu'un mot de passe pour se connecter au serveur SMTP. (on se connecte sur les ports 25, 587 avec authentification ou 465 sécurisé, avec envoi de mot de passe en clair ou crypté).

Si vous êtes connecté chez votre fournisseur d'accès, il n'est pas forcément nécessaire de se connecter au serveur SMTP avec un identifiant et mot de passe, car il vous connait: vous êtes déjà connecté sur son réseau, et quelque fois, il n'autorise la sortie que vers on propre serveur SMTP ! (la partie qui suit en gris et italique, est un peu plus technique, vous n'êtes pas obligé de la lire)

Dans ce cas, il se peut que vous soyez obligé d'utiliser le serveur SMTP de votre fournisseur d'accès plutôt que celui de votre boite aux lettres : Voici un petit exemple pour faciliter la compréhension de ce que je dis :

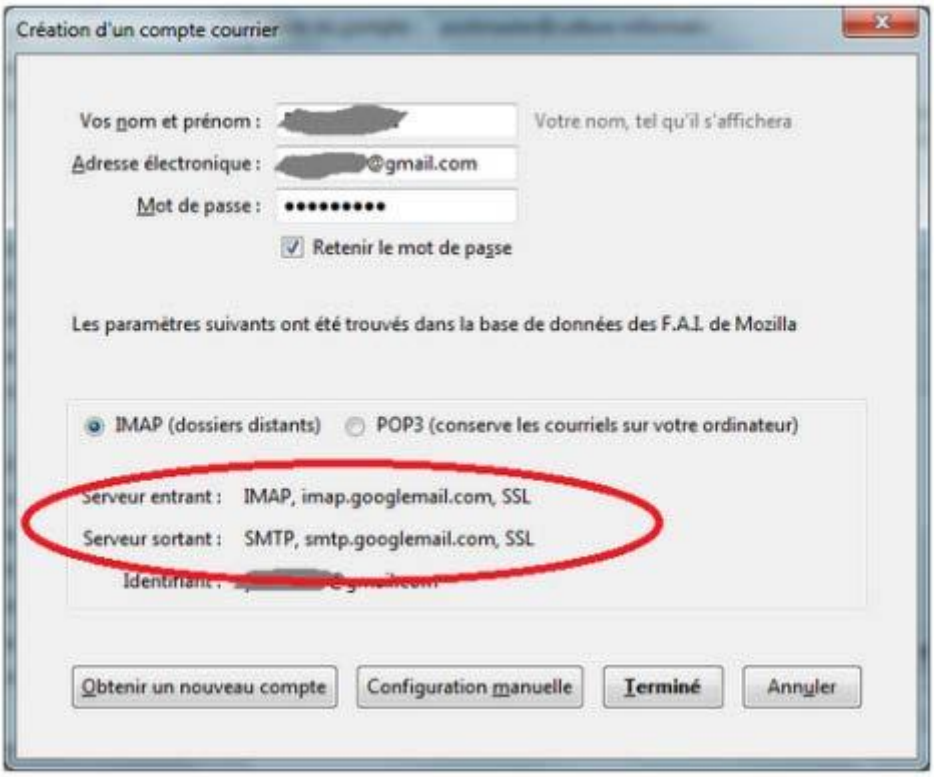
J'utilise une connexion chez le FAI Free, et je veux envoyer un mail avec mon adresse mail « xxx@orange.fr », et bien dans les paramètres de mon logiciel de messagerie, je vais mettre le serveur sortant : smtp.free.fr et non pas cela d'Orange !

La plupart des logiciels de messagerie (clients lourds tels que Outlook, ThunderBird, Incrédimail, Eudora, …) savent retrouver les serveurs en fonction de votre adresse mail. Dans quelques cas rares ou configurations particulières, vous pouvez avoir besoin de saisir les informations manuellement. (vous trouverez ces informations plus bas).

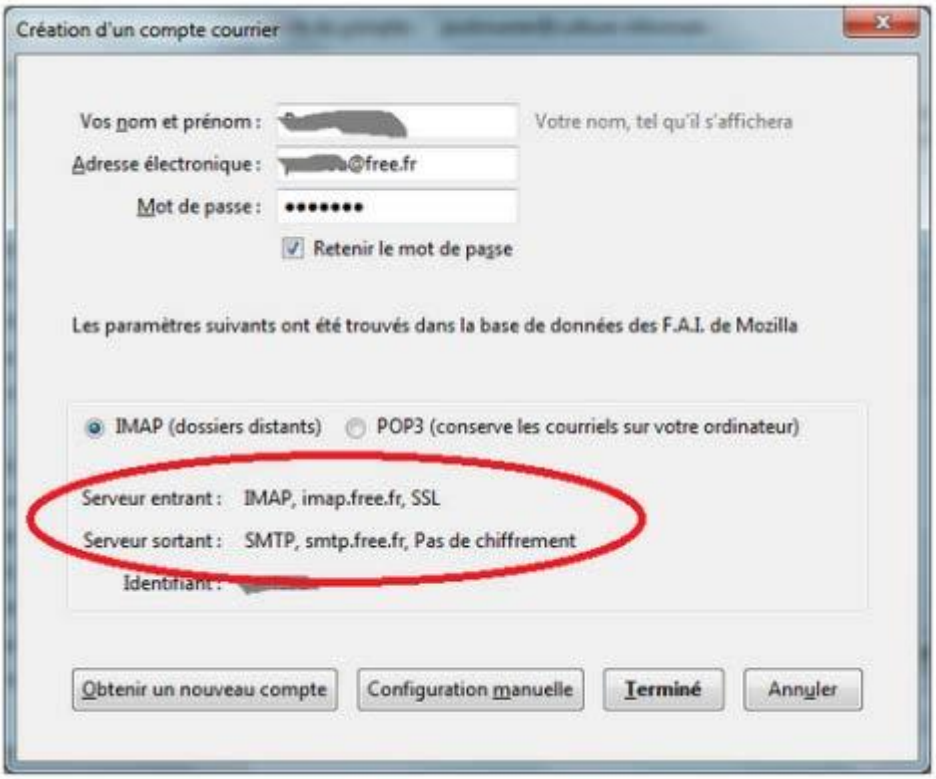
Tournez la page S.V.P

Voici des exemples des informations que retrouve automatiquement, le logiciel ThunderBird :

1. 1er exemple : avec une adresse chez gmail.com :



2. 2ème exemple, avec une adresse chez free.fr :



Comme vous pouvez le voir, sur la ligne serveur sortant SMTP
Thunderbird ne vous propose pas par défaut le protocole sécurisé (pas de chiffrement).
Si vous voulez un peu sécuriser vos envois de mails,
utilisez le même serveur smtp.free.fr mais avec le port 587 et mot de passe chiffré ! (voir ci-dessous)

Comme je vous le disais au-dessus, la plupart des clients lourds retrouvent les paramètres en fonction de l'adresse, mais si cela ne fonctionne pas ou que les paramètres ne vous conviennent pas.

[...]

Tournez la page S.V.P

Introduction à ITIL

ITIL (IT Information Library, traduisez bibliothèque de l'infrastructure des technologies de l'information) est un cadre de référence (en anglais framework) proposé par l'OGC (Office of Government Commerce) du Royaume-Uni rassemblant, dans un ensemble de guides, les meilleures pratiques en matière de management des services informatiques.La bibliothèque ITIL a été initiée dès le début des années 80 par le gouvernement britannique afin d'améliorer le service rendu par leurs directions informatiques.

L'objectif d'ITIL est de doter les directions des systèmes informatiques (DSI) d'outils et de documents leur permettant d'améliorer la qualité de leurs prestations, c'est-à-dire améliorer la satisfaction de leurs clients, tout en répondant au mieux aux objectifs stratégiques de l'organisation. Pour ce faire, l'approche consiste à considérer le Service informatique comme un ensemble de processus étroitement liés. Pragmatiquement, ITIL répond à la logique visant à faire en sorte que l'informatique soit au service du personnel et des clients et non l'inverse.

La démarche ITIL n'a pas comme seul bénéficiaires les directions informatiques puisqu'elle consiste à sensibiliser ces dernières sur le fait que la qualité et la disponibilité de l'infrastructure technologique a un impact direct sur la qualité globale de l'entreprise.

Le cadre ITIL

ITIL se décompose en neuf domaines, correspondant à neuf livres, permettant de couvrir l'ensemble des problématiques couvertes par les DSI. Les deux premiers (en gras) sont considérés comme le coeur de la méthode ITIL :

- **Service Support**
- **Service Delivery**
- Infrastructure Management
- Applications Management
- Service Management
- Business Perspective
- Business Requirements
- Technology

Service Support

Le domaine « Service Support » s'attache au fonctionnement et au support de l'infrastructure technologique. Il est décomposé selon les 6 processus suivants :

Processus	Objectif
Gestion des configurations	Geacute;rer l'infrastructure technologique en faisant un état des lieux de l'existant afin de mieux le gérer et le faire évoluer.
Gestion des incidents	Mieux détecter les incidents, améliorer le délai de résolution des incidents selon leur criticité sur le fonctionnement de l'entreprise.

Tournez la page S.V.P

Gestion des problèmes	Mieux gérer les problèmes récurrents et mettre en oeuvre des solutions de prévention afin de réduire leur occurence, voire les supprimer.
Gestion des changements	Mettre en oeuvre des démarches de conduite du changement afin d'anticiper les effets de bord.
Gestion des mises en oeuvre	S'assurer de l'adéquation du service avec les besoins métiers.
Gestion de la disponibilité	Assurer un niveau de disponibilité suffisant à un coût raisonnable.

Service Delivery

Le domaine « Service Delivery » .Il est décomposé en 4 processus comme suit :

Processus	Objectif
Gestion des niveaux de service	Maintenir un certain niveau de qualité de service grâce à des contrats de service renégociés périodiquement.
Gestion des capacités	Vérifier l'adéquation des capacités et performances avec les exigences actuelles et à venir.
Gestion de la continuité des services IT	Définir et mettre en oeuvre des délais contractuels pour la reprise après incident.
Gestion financière des services IT	Gérer la rentabilité des moyens mis en oeuvre pour fournir le service.

Bénéfices de la démarche ITIL

Etant donné que la démarche ITIL propose un référentiel des meilleures pratiques, les plus value de sa mise en oeuvre généralement constatées sont les suivants :

- Satisfaction des utilisateurs (personnel et clients),
- Clarification des rôles
- Amélioration de la communication inter-services
- Mise sous contrôle des processus avec des indicateurs pertinents et mesurables, permettant d'identifier les leviers pour réaliser des économies
- Meilleure compétitivité
- Sécurité accrue (disponibilité, fiabilité, intégrité)
- Capitalisation des données de l'entreprise
- Optimisation de l'utilisation des ressources
- Outil de parangonnage (benchmarking) et outil de positionnement vis-à-vis de la concurrence

Tournez la page S.V.P

Le rançongiciel

Qu'est-ce que c'est ?

C'est un programme malveillant, de type WannaCry ou Locky, qui provoque le blocage ou le chiffrement de tous vos fichiers d'ordinateur y compris ceux en partage en réseau.

Comment ça marche ?

Une rançon, en crypto-monnaie (monnaie utilisable sur un réseau informatique décentralisé) de type bitcoin la plupart du temps, vous est demandée en contrepartie du rétablissement de l'accès à l'ordinateur ou de la fourniture d'une clé de déchiffrement.

Cette méthode permet de masquer l'identité de l'attaquant et empêche toute poursuite judiciaire. De plus vous êtes mis sous pression puisqu'un chronomètre affiche le temps restant jusqu'à l'augmentation de la rançon, la destruction de vos données ou de leur diffusion en clair sur les réseaux.

Quel est son mode de propagation ? La diffusion de pièces jointes par courrier électronique reste le mode d'infection de plus courant ainsi que la mise à disposition d'un lien vers un site internet ayant une apparence authentique.

Comment se prémunir ?

Le facteur humain est déterminant puisque l'inattention de l'utilisateur conditionne la réussite de l'attaque. Vous devez être vigilant quant aux risques inhérents à l'ouverture de documents provenant d'émetteurs inconnus et/ou douteux.

- effectuez des sauvegardes fréquentes, ainsi en cas de chiffrement du disque dur, une restauration des données sera possible,
- évitez l'ouverture de pièces jointes de type SCR ou CAB,
- n'ouvrez pas vos courriels et ne naviguez pas depuis un compte ayant des autorisations « administrateur » mais privilégiez un compte utilisateur,
- utilisez un antivirus et mettez le régulièrement à jour, effectuez vos mises à jour logiciels et système.

Tournez la page S.V.P

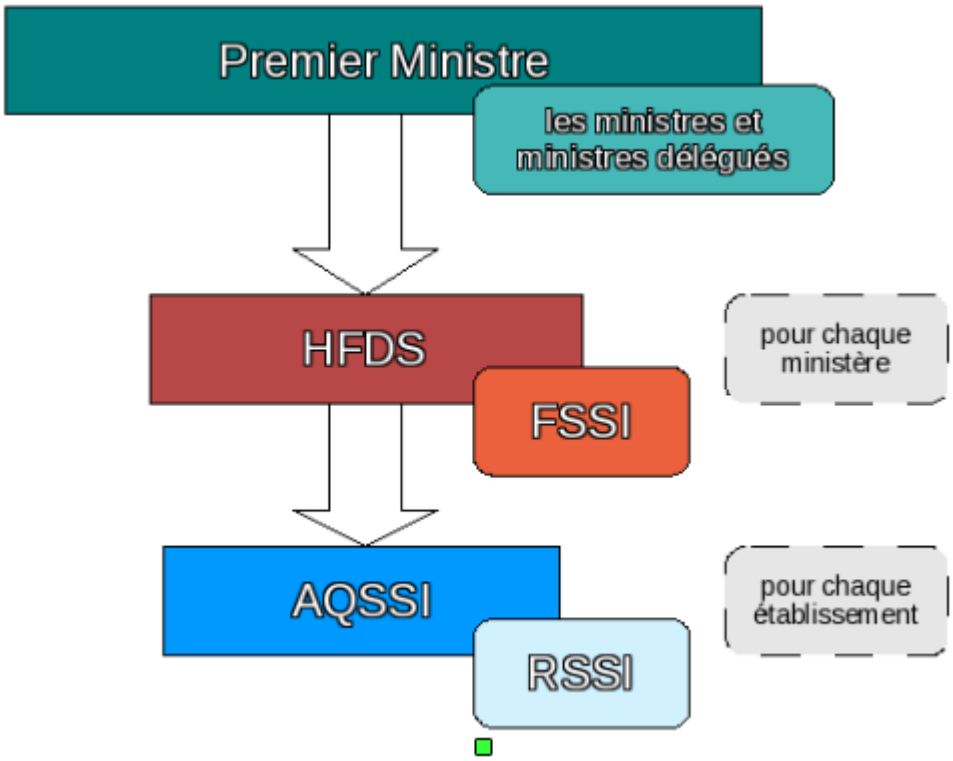
Que faire en cas d’incident ?

- déconnectez immédiatement votre poste de l’internet (arrêt du wi-fi, cable Ethernet débranché),
- ne payez pas la rançon car cette action ne garantie pas la récupération de vos données et serait un encouragement pour une nouvelle attaque,
- reformatez votre poste et installez un système sain.

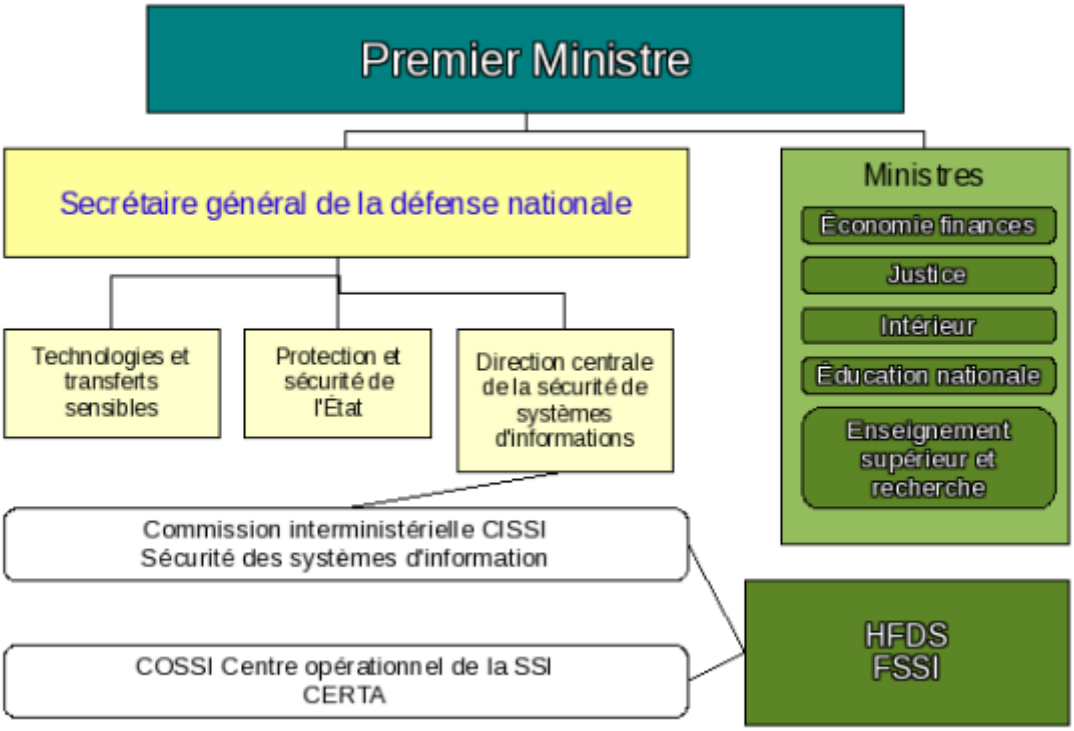
Tournez la page S.V.P

Le RSSI dans la chaîne fonctionnelle SSI

La chaîne fonctionnelle selon la recommandation interministérielle n°901



L'organisation interministérielle de la SSI



Tournez la page S.V.P

Les acteurs de la SSI

Les définitions suivantes sont tirées de la recommandation interministérielle n°901 et issues de la présentation de la chaîne fonctionnelle SSI au journées de CRSSI du CNRS 2007 par Isabelle Morel, ancien FSSI MEN/MESR.

HFDS – Haut fonctionnaire de défense et de sécurité

Définition :

« …est le conseiller du ministre pour toute question relative à la défense, la sécurité et la vie de la nation.» *Décret 2007-207 du 19 février 2007*

Son rôle :

- Animer et coordonner la préparation des mesures de défense, de vigilance, de prévention de crise et de situation d'urgence, et contrôler leur exécution
- Veiller à la protection du patrimoine scientifique et technique notamment en liaison avec les fonctionnaires de sécurité de défense (FSD)
- Animer la politique de sécurité des systèmes d'information et contrôler son application

FSD - Fonctionnaire de sécurité de défense

Définition :

Il est le correspondant du HFDS au niveau de chaque établissement d'enseignement supérieur et de chaque organisme de recherche.

Son rôle :

- La protection du patrimoine scientifique et technique
- La préparation et l'exécution des plans de défense et de sécurité
- La protection du secret

FSSI - Fonctionnaire de la sécurité des systèmes d'information

Définition :

« …un fonctionnaire de sécurité des systèmes d'information (FSSI) est désigné par le HFDS et placé sous son autorité…»

Son rôle :

- Porter la réglementation interministérielle relative à la SSI vers les AQSSI
- Participer à l'élaboration des politiques SSI et schémas directeur des grandes entités du ministère et en contrôler l'application
- Veiller à la coordination des flux de communication entre les différents acteurs ainsi qu'à la mutualisation des actions de formation, de sensibilisation et de retours d'expérience.
- Assurer la liaison avec les commissions interministérielles et ministérielles spécialisées en matière de SSI.

Tournez la page S.V.P

AQSSI - Autorités qualifiées pour la SSI

Définition :

« … autorités responsables de la SSI dans les administrations centrales et les services déconcentrés, ainsi que dans les établissements publics … »
« … Leur responsabilité ne peut pas se déléguer … » Dans les faits, il s'agit du chef d'établissement.

Son rôle :

- Définir une politique de sécurité des systèmes d'information adaptée à son organisme et en fixer les objectifs
- Assurer la responsabilité globale du niveau de sécurité requis
- Veiller à la mise en œuvre des dispositions réglementaires
- Procéder aux arbitrages et aux contrôles

RSSI (ASSI dans la circulaire)

Définition :

« … assistent les AQSSI »
« … chargés de la gestion et du suivi des moyens de sécurité des systèmes d'information se trouvant sur le ou les sites où s'exercent leurs responsabilités »

Son rôle :

- Seconder et conseiller les AQSSI. Ils doivent à ce titre avoir une connaissance de l'ensemble des activités des sites où s'exercent leurs responsabilités.
- Assurer le suivi des moyens nécessaires à la mise en oeuvre des consignes et directives définies par l'AQSSI à qui ils rendent compte.