IDEC école supérieure d'informatique

Brevet fédéral en informatique

Module 166-486

Définir et implémenter la sécurité des systèmes et des réseaux

Sommaire

Introduction

Nul n'oserait plus prétendre que la sécurité des systèmes d'information n'est pas l'un des objectifs majeurs que doit poursuivre l'exploitation IT. Car à quoi bon implémenter des technologies avancées pour améliorer la performance d'une entreprise si cela implique dans le même temps qu'elle encoure de nouveaux risques, capables non seulement de provoquer l'annulation des gains de performance obtenus mais, pire encore, de mettre en danger sa réputation, son patrimoine et de la placer dans l'illégalité ?

Comme l'explique le manuel du module 176 – Sécurité de l'information, les risques engendrés par une protection insuffisante du SI vont bien au-delà du problème informatique et ils doivent être pris en compte dès le niveau stratégique de l'organisation.

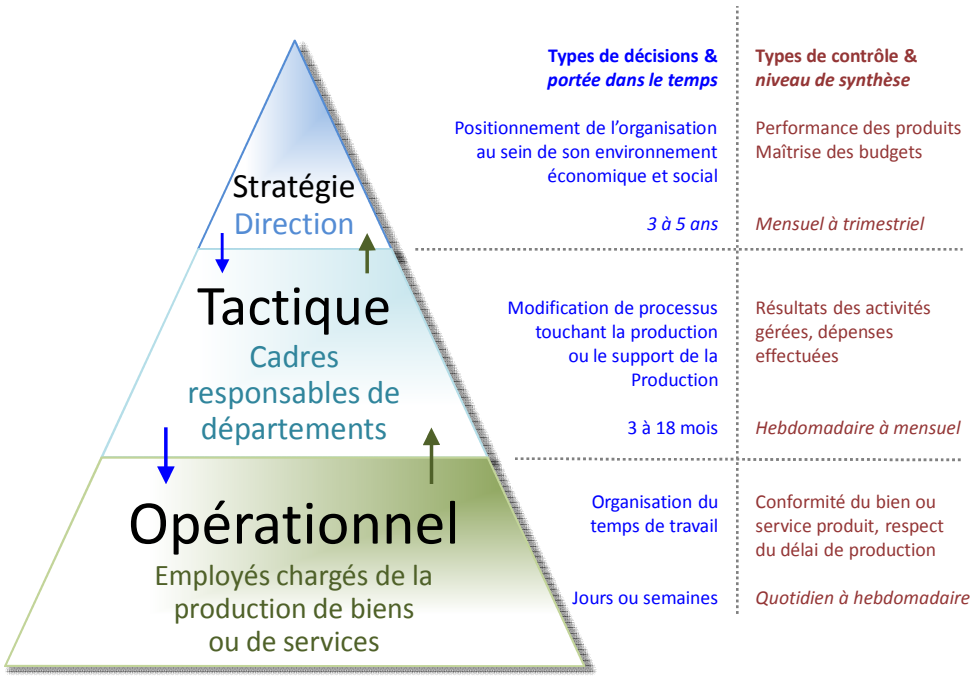


Figure 1 : la pyramide des objectifs de l'organisation

Dans la majorité des entreprises, une défaillance du SI peut se traduire :

- ☹ au niveau stratégique, par la perte de maîtrise du budget en cas de sinistre, l'incapacité à fournir la clientèle (réservation ou achat en ligne, délais garantis), l'atteinte à l'image de marque ou la diminution de la part de marché au profit d'un concurrent plus fiable,

- ☹ au niveau tactique, par des coûts supplémentaires générés par la correction d'erreurs, l'insatisfaction de la clientèle et la baisse de productivité des collaborateurs subissant des défauts de disponibilité ou d'intégrité des données,

- ☹ au niveau opérationnel, par des erreurs ou retards dans la production voire l'incapacité à effectuer les activités planifiées.

La sécurité des systèmes et des réseaux, qui constituent aujourd'hui une grande partie du système d'information, doit donc faire l'objet d'une véritable politique, tout comme une entreprise élabore sa politique commerciale ou une administration une politique de service public.

Figure 2 : la sécurisation du SI au travers de la pyramide décisionnelle

La définition des objectifs de sécurité, d'intégrité et de disponibilité, l'identification des actifs informationnels et des risques qu'ils courent font l'objet du module 176 – Assurer la sécurité de l'information, dont l'étude constitue un prérequis pour aborder le présent manuel.

Ce manuel, qui rassemble les compétences étroitement liées de deux modules[1] de brevet fédéral, concerne essentiellement le niveau opérationnel : une fois la politique de sécurité de l'information (PSI) définie, les risques évalués et la manière de les traiter décidée, vient l'étape de mise en œuvre concrète. Elle consiste à affiner le choix des mesures en fonction de l'analyse technique des vulnérabilités. C'est également au niveau opérationnel que l'on assure la surveillance constante du fonctionnement des mesures, que l'on réagit en cas d'incident et que l'on peut détecter la nécessité de mesures complémentaires.

Rappel

Un risque peut être géré de 3 façons : assumé, couvert ou transféré.

[1] 166 – Assurer la sécurité de base des TIC
486 – Implémenter des mesures de sécurité de réseau et de système

Ce manuel est organisé en trois grandes parties : la première décrit les vulnérabilités, la seconde les mesures de protection et la troisième propose une démarche méthodologique pour réaliser l'inventaire des unes et positionner les autres.

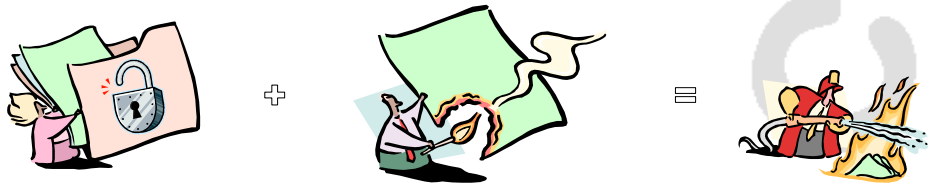
1. Les vulnérabilités

Les vulnérabilités sont les éléments liés au SI (matériels, logiciels, réseaux, personnes) ou à l'entreprise (activité, modèle d'organisation, implantation géographique, partenaires externes, etc.) qui induisent des risques de perte de confidentialité, d'intégrité, de disponibilité et de traçabilité.

Une vulnérabilité constitue un risque s'il existe une menace capable de l'exploiter. Une menace peut être soit un acte volontaire utilisant un

moyen d'exploiter la vulnérabilité (piratage, intrusion, virus…), soit un événement relevant du hasard (panne, erreur humaine…)

Un sinistre se produit quand une menace rencontre une vulnérabilité :



vulnérabilité + *menace : événement ou intention nuisibles* = *sinistre*

Rappel

L'association d'une catégorie de vulnérabilité avec un type de menace est appelé risque (ou scénario de risque)

Chaque vulnérabilité décrite ci-après est identifiée[2] par un type (utilisateur, logiciel, …) et un numéro qui seront utilisés dans le tableau indiquant les mesures permettant de la supprimer ou de l'atténuer 187. Les principales menaces basées sur l'exploitation de la vulnérabilité sont précisées ainsi que les conséquences les plus fréquentes.

Les domaines de conséquences – confidentialité, intégrité, disponibilité – auxquels elle appartient sont également indiqués, sous forme graphique en regard de chaque vulnérabilité :

C I D perte de confidentialité, d'intégrité et de disponibilité

C I D perte de confidentialité et d'intégrité

C I **D** perte de disponibilité

Les vulnérabilités sont décrites par domaine d'origine – utilisateur, organisation, réseau, logiciel, matériel – afin de faciliter la sélection des mesures.

[2] cette identification n'existe que pour faciliter l'usage du présent manuel et ne découle d'aucune norme, elle ne doit pas être utilisée en dehors du contexte de ce manuel.

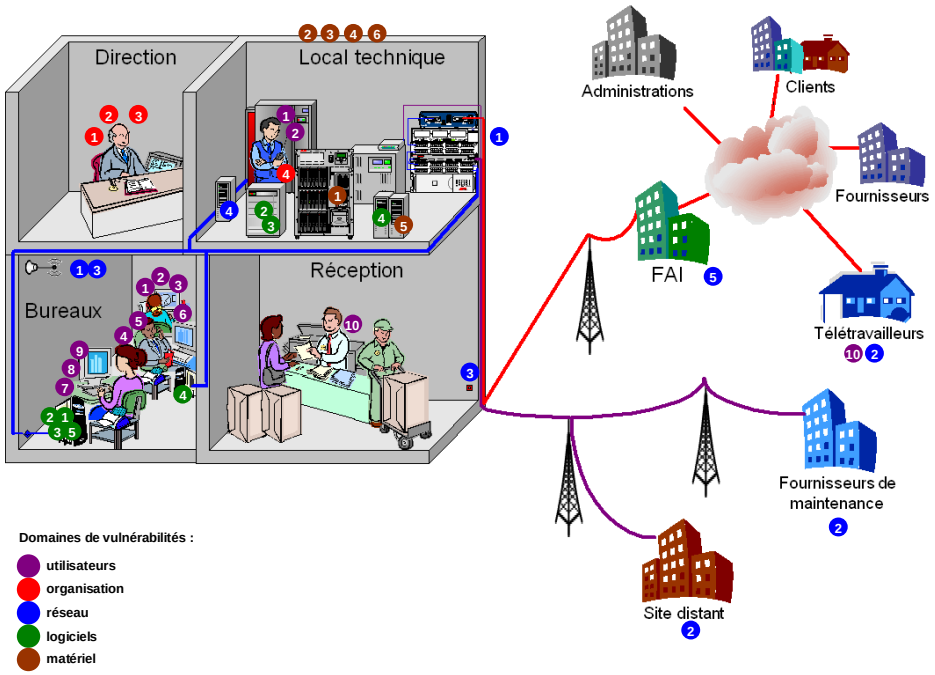


Figure 3 : répartition des vulnérabilités principales par domaine d'origine

1.1 Utilisateurs

L'utilisateur est la raison d'être du SI. Les opérations réalisées par le système informatique le sont à sa demande, directe ou indirecte. L'utilisateur est donc le détenteur du pouvoir et, à ce titre, il représente aussi la plus grande menace pour le SI.

Certains considéreront que les vulnérabilités citées ci-après ne sont pas relatives à l'utilisateur mais au logiciel, qui doit sécuriser les actions de l'utilisateur. Bien que souvent employée, cette approche n'est qu'un pis-aller et non une solution : ce n'est pas à l'outil de décider comment il doit être utilisé.

Sécuriser le logiciel pour protéger le SI de l'utilisateur va à l'encontre de la raison d'être du système : ce dernier doit être au service de l'utilisateur, et non l'inverse.

L'utilisateur doit conserver son pouvoir de décision quant aux opérations qu'il effectue sur le système : laisser décider le logiciel ne serait possible que s'il pouvait connaître tous les besoins et chaque intention de l'utilisateur… Comme tous les outils puissants, l'informatique peut être

aussi un outil dangereux. Former les utilisateurs à s'en servir en respectant des normes de sécurité est une solution bien meilleure que limiter les fonctionnalités de l'outil… Votre voiture conduit-elle à votre place parce que vos actions pourraient provoquer un accident ?

VU1 – Erreurs d'utilisation

C I D

Figurant régulièrement dans les premières places du classement des causes de sinistres, les erreurs d'utilisation peuvent être dues soit au manque de formation (l'utilisateur pense effectuer l'opération correctement), soit au manque de contrôle (l'utilisateur fait une fausse manipulation).

Principales menaces :

- suppression involontaire de fichier : opérations d'effacement validées trop rapidement ou remplacement par un fichier de même nom mais de contenu différent, déplacement involontaire de fichiers (*drag & drop*) : si l'utilisateur ne s'en aperçoit pas, le fichier sera considéré comme perdu lors de sa prochaine utilisation, alors qu'il se trouve simplement dans un autre répertoire.

- activation d'une fonction au lieu d'une autre : certains traitements ne peuvent pas être annulés, de plus, l'utilisateur ne réalise pas toujours son erreur à temps,

- modification d'un autre champ ou texte que celui qui devait être modifié,

- opérations de presse-papier : couper sans coller, collage involontaire d'informations confidentielles dans une zone inappropriée.

Les professionnels de l'informatique commettent aussi des erreurs et elles sont plus graves car leurs privilèges sont plus élevés et leur domaine d'intervention plus vaste. Parmi les erreurs courantes, on citera :

- mauvaise configuration de sauvegardes et/ou de restaurations : on écrase la version récente avec la copie de sauvegarde,