Pélissier Thomas

Mouzouri Naoual

Jebara Karim

Master 2 MIAGE

Solutions matérielles de double authentification



Monsieur Courtaud 2015/2016

Table des matières

**Introduction**   
  
La démocratisation de l’utilisation d’internet a conduit les entreprises à ouvrir leur système d’information aussi bien pour leurs clients, partenaires et fournisseurs. La question de la sécurité se pose alors pour les entreprises.

Il est absolument nécessaire à l’entreprise de définir toutes les ressources sensibles de l’entreprise afin de les protéger et maîtriser le contrôle d’accès à ces informations. Pour cela, l’entreprise doit en amont mettre en place une solution de droits des utilisateurs sur son système d’information.

Cette politique de droits doit par la suite être étendue lors de l’ouverture du système d’information avec l’extérieur par le biais d’Internet.

Plus récemment, l’apparition des ordinateurs portables a conduit les entreprises à sécuriser l’ensemble de son infrastructure informatique. Dans le cas où l’ordinateur portable d’un collaborateur de la société venait à tomber dans les mains d’un concurrent, si ce dernier n’est pas sécurisé, toutes les informations seront visibles par ce dernier. On peut facilement imaginer les conséquences néfastes pour l’entreprise.

1. La sécurité informatique
   1. Définition

Toutes entreprises disposent à ce jour d’un système informatique. Celui-ci permet de collecter, stocker, traiter et diffuser de l’information dans l’objectif de répondre aux besoins du cœur de métier de l’entreprise.

Comme énoncé dans l’introduction, le système informatique d’une entreprise est vulnérable depuis l’extérieur par le biais d’internet mais il l’est également depuis l’intérieur.

La sécurité informatique, comme son nom l’indique, permet de sécuriser un système informatique. Ceci dans l’optique de limiter au maximum le risque[[1]](#footnote-1) de menaces[[2]](#footnote-2) d’attaques, on dit dans ce contexte qu’un système est vulnérable[[3]](#footnote-3). Afin de prévenir la menace, une entreprise doit mettre en place un ensemble de contre-mesures[[4]](#footnote-4).

Les entreprises appliquent deux types de contre-mesures :

* Mettre en place des procédures afin de sécuriser l’infrastructure informatique
* Former et sensibiliser les collaborateurs sur les menaces.

Dans l’optique de sécuriser son système informatique, l’entreprise se doit en amont d’identifier les menaces possibles. En fonction de cette identification, l’entreprise doit mettre en place les contre-mesures nécessaires.

* 1. Finalité de la sécurité informatique

L’objectif de la sécurité informatique est d’assurer que les ressources aussi bien matérielles que logicielles sont employées uniquement dans l’entreprise et le cadre de son cœur de métier. Elle permet de protéger le patrimoine de l’entreprise.

La sécurité informatique permet de répondre aux objectifs suivants concernant les données :

* La disponibilité : L’entreprise doit définir le moment de la journée ou les informations doivent être impérativement disponibles. Certaines informations devront être disponibles pendant le temps de travail, d’autres toute la journée. Une fois cette définition réalisée, le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
* L’intégrité : On s’assure que le traitement, la conservation et la transmission des données ne subissent aucune destruction volontaire ou accidentelle et aucune altération.
* La confidentialité : Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
* La traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
* L’authentification : L'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
* La non-répudation : Aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées, et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.
  1. Démarche à entreprendre

La démarche générale pour l’entreprise consistant à mettre en place une sécurité du système d’information est la suivante :

1. Définir et évaluer les risques et leur criticité[[5]](#footnote-5). C’est-à-dire en fonction de chaque type de donnée définir quels sont les risques, les menaces et quelles sont les conséquences en cas de pertes de cette donnée.
2. Déterminer et adopter les contre-mesures à mettre en place. On doit se poser la question que doit-on sécuriser et comment.
3. Appliquer et tester les contre-mesures misent en place.

Une fois les contre-mesures misent en place, cela ne suffit pas pour garantir une sécurité du système. Il faut impérativement vérifier régulièrement les contre-mesures en réalisant des tests, s’adapter en fonction des nouvelles méthodes d’attaques.

* 1. Identification des menaces

Nous avons caractérisé quatre sources de menaces auxquelles le système d’information peut être confronté :

1. L’entreprise peut être soumise à l’endommagement de matériels informatique du un sinistre (vol, incendie, dégât des eaux, …). Dans ce type de situation, les données sont généralement perdues.
2. Un utilisateur du système d’information peut être en péril intentionnellement ou non la sécurité du système d’information.
3. Un programme malveillant installé par un utilisateur du système par mégarde ou non peut conduire à créer des failles de sécurité dans le système.
4. Une personne extérieur (hacker) à l’entreprise qui parvient à percer toutes les protections du système et arrive par conséquent à s’y introduire et avoir accès aux données.
   1. Identification des dommages

Nous avons analysé quatre types de dommages que peut rencontrer une entreprise en cas de manquement en termes de sécurité de son système d’information :

1. Des dommages de types financiers :
   1. Soit sous forme de dommages de coûts directs, c’est-à-dire le remplacement de matériels suite à un sinistre, la reconstitution de données perdues, …
   2. Sois sous forme de dommages de coûts indirects, c’est-à-dire le vol d’un secret de fabrication, de plan stratégique d’investissement futur de l’entreprise, …
2. Suite à une attaque, l’image de marque de l’entreprise sera affaiblie.
   1. Affaiblissement directe suite à une publicité négative faite par la publication de l’attaque.
   2. Affaiblissement indirecte par la baisse voire la perte de confiance des consommateurs.
3. Des dommages par non respecté légale de la disponibilité des données. L’indisponibilité d’un système d’informations peut conduire l’entreprise à une situation de défaut face à ses obligations légales et juridiques.
4. Des dommages écologiques et sanitaires : Une panne du système d’informations peut conduire à des catastrophes écologies et/ou sanitaires.

Webographie

<https://fr.wikipedia.org/wiki/Authentification_forte>

<https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d'information>

<http://www.ssi.gouv.fr/uploads/IMG/pdf/mementodep-v1-1.pdf>

<http://www.cnil.fr/vos-obligations/vos-obligations/>

<http://www.intrapole.com/spip.php?article18>

<http://www.commentcamarche.net/contents/1033-introduction-a-la-securite-informatique>

<http://www.ssi.gouv.fr/particulier/>

1. On définit le risque par l’équation suivante : Risque = ( Menace X Vulnérabilité ) / ( Contre-Mesure) [↑](#footnote-ref-1)
2. La menace représente une action capable de nuire à l’activité de l’entreprise. [↑](#footnote-ref-2)
3. La vulnérabilité est le niveau d’exposition face à la menace d’un système informatique. [↑](#footnote-ref-3)
4. La contre-mesure est l’ensemble des actions mises en œuvre en prévention de la menace. [↑](#footnote-ref-4)
5. La criticité est la détermination et hiérarchisation du degré d’importance et de la disponibilité du système d’information. [↑](#footnote-ref-5)