# CHAPITRE 1 : INTRODUCTION

## I. Introduction générale :

Aujourd'hui et suite au développement de l'internet et de la technologie des TIC, de plus en plus d'entreprises sont confrontées à l'obligation de faire ouvrir leur SI à leurs partenaires. Ainsi, la sécurité est devenue un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent, et elle n'est plus confinée uniquement au rôle de l'informaticien.

Sa finalité sur le long terme est de ***maintenir la confiance des utilisateurs et des clients***. La finalité sur le moyen terme est la ***cohérence de l'ensemble du système d'information***. Sur le court terme, l'objectif est que ***chacun ait accès aux informations dont il a besoin dans des meilleures conditions***.

## Historique :

Les responsables de systèmes d'information se préoccupent depuis longtemps de sécuriser les données. Le cas le plus répandu, et sans aucun doute précurseur en matière de sécurité de l'information, reste la sécurisation de l'information stratégique et militaire. Le ***Department of Defense*** (***DoD***) des États-Unis est à l'origine du ***TCSEC*** (*Trusted Computer System Evaluation Criteria*), la norme américaine qui définit les règles et les critères de la sécurité.

Cette norme a été publiée la 1ère fois en 1985 dans un ouvrage (*orange book*) et qui été mise à jours plusieurs fois dans la suite. Les critères majeurs sur lesquels porte cette norme sont la confidentialité et l'intégrité de données et la disponibilité du système. Pour en arriver à assurer ces critères, cette norme a défini les fonctionnalités de sécurité suivantes : contrôle d'accès, imputabilité (identification et authentification), assurance d'architecture, intégrité du système, test de sécurité documentations, réutilisation des objets, et audit de sécurité.

Cette norme a bien fait l'accent sur le principe de "***sécurité multi-niveaux***", et ce en définissant 4 niveaux de sécurité (chacun peut être réparti en plusieurs classes) :

- Niveau D : « ***Minimal Protection*** » contenant les systèmes qui n'ont pas pu satisfaire aux exigences de classe de niveau supérieur.
- Niveau $C_1/C_2$ « ***Discretionary protection*** » : Protections laissées à la discrétion des utilisateurs. $C_2$ est le niveau maximum pour les organismes commerciaux.
- Niveau $B_1/B_2/B_3$ : « ***Mandatory protection*** » et Niveau A : « ***Verified protection*** » : Ces niveaux couvrent essentiellement les besoins militaires, ou d'autres domaines sensibles comme le transport aérien. L'accès aux informations (objets) est règlementé par les habilitations des sujets selon les 2 axes suivants :

La norme européenne ITSEC (*Information Technologie Security Evaluation Criteria*) définit l'ensemble machine/logiciel comme cible d'évaluation. Les fonctionnalités de sécurité sont désignées sous le terme de cible de sécurité. Au-delà des fonctionnalités déjà expliquées dans la norme américaine, celle-ci a ajouté le principe de fidélité (détection et prévention de perte et altération de données), continuité de service et sécurisation des canaux de communications.

Ces deux normes ainsi que la norme canadienne CTCPEC (*Canadian Trusted Computer Product Computer Product Evaluation Criteria*) ont été réunies plus tard pour créer la norme ISO 15408 en 1999.

De même, le principe de la ***défense en profondeur*** (technique militaire destinée à retarder l'ennemi), est toujours d'actualité aujourd'hui ; elle consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant.

Aujourd'hui, il est généralement admis que la ***sécurité ne peut être garantie à 100 %*** et requiert donc le plus souvent la mobilisation d'une panoplie de mesures pour réduire les chances de pénétration des systèmes d'information.

## *Enjeux de la sécurité des systèmes d'information :*

Le terme « **système informatique** » désigne ici tout système dont le fonctionnement fait appel, d'une façon ou d'une autre, à l'électricité et destiné à **élaborer**, **traiter**, **stocker**, **acheminer** ou **présenter** de **l'information**. Les systèmes d'information s'appuient en règle générale sur des systèmes informatiques pour leur mise en œuvre. Ils comprennent les données de télécommunications (voix analogique, voix sur IP…) et dans certains cas, les données sur papier.

De tels systèmes se prêtent à des menaces de types **divers**, susceptibles **d'altérer** ou de **détruire** l'information (**intégrité**), ou de la **révéler** à des tiers qui ne doivent pas en avoir connaissance (**confidentialité**), ou bien par exemple de porter atteinte à en **accéder** (**disponibilité**).

Depuis les années 1970, **l'accès** rapide aux informations, la **rapidité** et **l'efficacité** des traitements, les **partages** de données et **l'interactivité** ont augmenté de façon considérable — mais c'est également le cas des **pannes — indisponibilités**, **incidents**, **erreurs**, **négligences** et **malveillances** en particulier avec l'ouverture sur internet.

Certaines de ces menaces peuvent aussi, indirectement, causer d'importants dommages **financiers**. Par exemple, bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars US ont été avancées suite à des dommages causés par des programmes malveillants comme le ver ***Code Red***. D'autres dommages substantiels, comme ceux liés au vol de numéros de cartes de crédit, ont été déterminés plus précisément.

Outre les aspects financiers, des bris de sécurité informatique peuvent causer du tort à la **vie privée** d'une personne en diffusant des informations confidentielles sur elle (entre autres ses coordonnées postales ou bancaires), et peuvent pour cette raison être sanctionnés lorsqu'une négligence de l'hébergeur est établie : si, par exemple, celui-ci n'a pas appliqué un correctif dans des délais raisonnables.

Indirectement aussi, certaines menaces peuvent nuire à **l'image** même du propriétaire du système d'information. Des techniques répandues de « ***defacing*** » (une refonte d'un site web) permettent à une personne mal intentionnée de mettre en évidence des failles de sécurité sur un serveur web. Ces personnes peuvent aussi profiter de ces vulnérabilités pour diffuser de fausses informations sur son propriétaire (on parle alors de désinformation).

**Exemples d'incidents :**

- Virus Slammer (376 caractères, capable d'attaquer 55 millions d'ordinateurs par seconde) a été repéré pour la 1ère fois le 25/01/2003 à 6h30. Une fois un ordinateur est contaminé, on ne pouvait accéder à aucune page web ou recevoir d'email. De nombreux services de par le monde se sont retrouvés en panne : contrôle aérien, distributeurs de billets, paiement par carte bancaire. La perturbation a duré toute la journée du 25 janvier.
- En mars 2005 la police de Londres découvre une des plus grandes tentatives de vol au Royaume-Uni dans la banque Chinoise Sumitomo Mitsui, qui a été cible pendant plusieurs mois d'un gang de pirates qui utilisaient des Keylogger. Leur plan déjoué de justesse prévoyait le transfert de 220 millions de livres sterling.
- La catastrophe de la navette spatiale Ariane 5 en 1996 (bogue dans son système).
- Espionnage industriel chez Valeo en 2005.
- Des internautes français ont été victimes d'assaut de pirates russes en 2006 (estimation 1 million d'euro a été dérobée grâce à un cheval de Troie volant les identifiants.
- Destruction d'un disque dur d'un serveur lors d'une opération de maintenances d'une grande PME (estimation du coût plus de 100000 euro).

## *Embarras et conséquences de l'insécurité :*

La sécurité informatique est un défi d'ensemble et concerne : Les infrastructures matérielles de traitement ou de communication, les logiciels (systèmes d'exploitation ou applicatifs), les données, le comportement des utilisateurs etc..

***Le niveau global de sécurité étant défini par le niveau de sécurité du maillon le plus faible***, les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Plusieurs types de dommages peuvent affecter le système d'information d'une organisation :

- **Des dommages financiers :** Dommages directs (comme le fait d'avoir à **reconstituer** des bases de données qui ont disparu, **reconfigurer** un parc de postes informatiques, **réécrire** une application) ou indirect par exemple (le **dédommagement** des victimes d'un piratage, le **vol** d'un secret de fabrication ou la **perte de marchés commerciaux**). Un exemple concret : bien qu'il soit relativement difficile de les estimer, des sommes de l'ordre de plusieurs milliards de dollars US ont été avancées suite à des dommages causés par des programmes malveillants comme le ver **Code Red**. D'autres dommages substantiels, comme ceux liés au vol de numéros de cartes de crédit, ont été déterminés plus précisément.
- **La perte ou la baisse de l'image de marque** : Perte directe par la publicité négative faite autour d'une sécurité insuffisante (cas du hameçonnage par exemple) ou perte indirecte par la baisse de confiance du public dans une société. Par exemple, les techniques répandues de ***defacing*** (une refonte d'un site web) permettent à une personne mal intentionnée de mettre en évidence des failles de sécurité sur un serveur web. Ces personnes peuvent aussi profiter de ces vulnérabilités pour diffuser de fausses informations sur son propriétaire (on parle alors de désinformation).
- **Des pertes morales** : Les conséquences peuvent aussi concerner la vie privée d'une ou plusieurs personnes, notamment par la diffusion d'informations confidentielles.

## *Impact financier :*

Les dépenses gouvernementales **en services et produits de sécurisation des données** sont vraiment considérables, et elles augmentent sans cesse. Les dépenses de l'administration américaine dans les dernières années sont estimées à :

- 2009 : 7,9 milliards de $
- 2010 : 8,3 milliards de $
- 2011 : 9 milliards de $
- 2012 : 9,8 milliards de $
- 2013 : 10,7 milliards de $
- 2014 : 11,7 milliards de $
- 2016 : 35 milliards de $

A l'échelle mondiale l'entreprise américaine de conseil ***Gartner*** estime que ces dépenses atteindront la somme de 84,4 milliards de dollars en 2017 (93 milliards dans la réalité), suite à une augmentation de 7% en 2016, et un chiffre attendu de 93 milliards de dollars en 2018 (103 milliards dans la réalité).

# *Résumé :*

## *1) Les ressources à protéger dans un SI ?*

L'être humain ? Les bâtisses (immeubles) ? Les ressources matérielles ? L'information ?

La sécurité des ressources humaines, bâtisses et matériel est généralement (voir quasiment) étudiée dans le plan de sécurité général qui nécessite une sécurité physique (normes de construction de bâtisses, plan de protection et secours contre incendie, inondation, séisme etc..).

- Or la ressource essentielle dans un SI est ***l'information***, il est donc très important de garantir sa ***disponibilité***, son ***intégrité*** et sa ***confidentialité***.

## *2) Niveau de sécurité :*

Niveau de sécurité global d'un système est égal à celui le plus bas des composants de ce système. (la sécurité ressemble à une chaine).

## *3) Caractéristiques :*

- La sécurité du SI n'est pas une question conjoncturelle à laquelle on alloue du temps et des ressources à chaque fois qu'un incident lié à la sécurité des systèmes se déclare. Il faut se doter d'une ***démarche claire*** et ***structurée*** pour la mise en place et la mise à niveau de la sécurité SI.
- La sécurité du SI doit être multi-niveaux selon le ***type d'utilisateur*** et leurs droits d'accès, ***l'importance des biens*** à protéger, l'endroit et l'environnement ***d'accès*** etc.
- La sécurité à ***100% n'existe pas*** et n'existerai jamais.
- La sécurité ***évolue*** dans le ***temps*** selon l'évolution technologique et l'environnement.
- La sécurité ne doit pas se baser sur des solutions ***techniques uniquement*** (solution technique, organisationnelle, procédurale, et juridique).
- Le processus de sécurisation d'un système doit se baser sur le principe de ***défense en profondeur*** : chaque composant dans le système doit avoir son propre mécanisme de sécurisation en plus de la sécurisation du système global (ces mécanismes doivent être plus ou moins différents).

## *4) Vision (objectifs) :*

Le processus de sécurisation du SI vise à :

- Au long terme à gagner et maintenir la confiance de ses partenaires (utilisateurs et clients).
- Au moyen terme à garantir le bon fonctionnement du système et la cohérence des tâches effectuées.
- A court terme à garantir l'accès des utilisateurs aux ressources dont ils ont besoin dans des meilleures conditions (temporelle, qualité de services, ..)

## *5) Pourquoi sécuriser ?*

Les risques de l'insécurité peuvent être catastrophiques :

- Pertes financières.
- Perte de l'image de marque.
- Pertes morales.

## *6) Contre qui (quoi) ?*

- Menaces humaines : accident, attaque, vol, erreur, accès non autorisé, …
- Menaces informatiques (logicielle et matérielle) : virus, cheval de Troie, etc.
- Menaces naturelles : catastrophes naturelles (séisme, inondation, incendie, etc..)

### 7) Quand ?

Les responsables ne pensent généralement à la sécurité que lorsqu'un évènement lié à la sécurité fait la une des journaux. Cependant la sécurité ne doit jamais être une question conjoncturelle ; c'est plutôt une démarche (stratégie) continue qui vit et évolue avec l'évolution du système et de la technologie.

### 8) Comment ?

Si les décideurs sont sensibilisés sur la sécurité de l'information, ils sont rapidement affrontés à la problématique du 'Comment'. En effet il n'a y pas de solution 'CLEF EN MAIN' qui offre une sécurité parfaite du système d'information et ce du fait que :

- L'information n'est pas toujours numérique, elle peut être sur un support papier ou non documentée ;
- Les risques ne sont pas toujours externes. En effet, une grande partie du risque vient souvent de l'interne ;
- La SSI dépasse les limites de la sécurité informatique et concerne d'autres volets : sécurité physique, sécurité de l'environnement, continuité d'activité, … .

# II. Définitions :

## 1. Sécurité des systèmes d'information SSI :

La sécurité du système d'information (SSI) est la qualité d'être protégé contre tous genres d'abus d'information suite à des menaces accidentelles ou intentionnelles, en allant de la minimisation des vulnérabilités du système (à l'état absolu) jusqu'au rétablissement de l'état du système (entièrement ou partiellement) en cas d'incidents.

Elle nécessite ainsi la mise en place d'un ensemble des moyens techniques, organisationnels, juridiques et humains pour conserver, rétablir, et garantir la sécurité du système d'information.

Assurer la sécurité du système d'information est une activité du management du système d'information. Elle n'est plus confinée au rôle de l'informaticien mais plutôt c'est le rôle de l'ensemble des acteurs de l'entreprise.

Son objectif sur le long terme est de maintenir la confiance des utilisateurs et des clients, sur le moyen terme est la cohérence de l'ensemble du système d'information, sur le court terme, l'objectif est que chacun ait accès aux informations dont il a besoin.

En anglais on utilise deux termes différents pour séparer entre les deux aspects de la sécurité :

### a. Sécurité = " Safety" (sécurité-innocuité) :

Protection des systèmes informatiques contre les accidents dus à l'environnement, les défauts du système (bogues/failles) et les défauts des êtres humains (erreur/accidents).

Domaine d'élection : les systèmes informatiques contrôlant des procédés temps réels et mettant en danger des vies humaines (transports, énergie, santé, ..)

### b. Sécurité = "Security"

Protection des systèmes informatiques contre des actions malveillantes intentionnelles.

Domaine d'élection : les systèmes informatiques réalisant des traitements sensibles ou comprenant des données sensibles (banques, centres de recherches, …).

## 2. Menace (Threat) :

C'est tout type d'action susceptible de nuire dans l'absolu que ce soit par intention ou par accident, et qui provient de l'intérieur du système ou de son environnement extérieur

(pannes, accidents, sinistres, catastrophes, erreurs humaines, malveillances internes et attaques externes).

## 3. Vulnérabilité :

Appelée aussi "Faille" ou "Brèche" représente le niveau d'exposition face à la menace dans un contexte particulier. Elle peut être de différents types :

- Faille technique (bug d'application, système, protocole ou équipement).
- Faille humaine (faiblesse, fatigue, laxité, maladie, non sensibilisation,...).
- Faille d'organisation.
- Faille de procédure de travail.

## 4. Contre-mesure :

Ce sont l'ensemble des techniques et moyens (informatique ou non informatique) mis en place en prévention d'une menace. Ces mesures doivent être de différents aspects :

- Solution technique.
- Solution organisationnelle.
- Solution juridique.

## 5. Risque :

Possibilité qu'une menace exploite une vulnérabilité et crée un impact. En termes de sécurité il est généralement caractérisé par l'équation suivante :

$$\text{Risque} = \frac{\text{Menace} * \text{ Vulnérabilité}}{\text{Contre} - \text{mesure}}$$

On appelle ***Risque résiduel*** le risque qui subsiste après application des précautions et contre-mesures servant à réduire le risque.

### Exemples :

- Les biens sont **sensibles à des menaces** telles que les accidents, les erreurs, les négligences ou les malveillances.
- Ces menaces sont **liées à des vulnérabilités** du système d'information (bogues, faille, absence ou méconnaissance des règles, etc.).
- Le risque est la possibilité qu'une de ces menaces exploite l'une de ces vulnérabilités et crée un impact sur ces biens.

### Exemple 1 :

Un document confidentiel est dans une armoire non fermée à clef.

- **Le bien** : le document confidentiel.
- **La vulnérabilité** : une armoire non fermée à clef.
- **Contre-mesure :** armoire non fermée à clef.
- **Une menace** : le vol du document.
- **Le risque** c'est l'opportunité du vol de ce document confidentiel en exploitant le non fermeture de l'armoire à clef.

### Exemple 2 :

Un cambrioleur tente d'entrer par une porte fermée à clef mais la clef est cachée au-dessous d'un tapi devant la porte; en essayant différentes clés sans résultat il découvre la clef cachée.

- **Le bien** : l'argent.
- **Vulnérabilité** : clé mal cachée.
- **Contre-mesure :** porte fermée à clef.
- **Une menace** : vol de l'argent.
- **Risque** : valeur de l'argent volée en ouvrant la porte par la clef.
- **Risque résiduel** : valeur de l'argent volée suite à : clé volée par un Pickpocket ou perdue, ou bien vol par effraction (casser la porte par un arrache-clou).

### *L'appréciation des risques*

L'appréciation du risque consiste à l'évaluer en fonction :

- de sa **vraisemblance** : quelle est la probabilité que le danger survienne ?
- des dommages ou **impacts** qu'il est susceptible de provoquer sur les valeurs essentielles (atteintes juridiques, perte d'image, etc.). On parle aussi de la **gravité** du risque.

Identifier les biens à protéger, apprécier les risques qui pèsent sur ces derniers permet de mettre les investissements, les exigences et les contraintes là où ils sont incontournables.

Pour être comprises et acceptées, les mesures de sécurité doivent être adaptées et répondre aux besoins de l'organisation.

## *III. Objectif de la sécurité de l'information :*

La ressource principale concernée par le sujet de sécurité des SI est l'information, bien que la sécurité des autres ressources est aussi importante (êtres humains, battisses,..) que celle de l'information, mais elle est étudiée dans le plan de sécurité général (normes de construction de bâtisses, plan de protection et secours contre incendie, inondation, séisme etc..).

Ainsi la sécurité de l'information dans un SI doit viser les objectifs suivants :

- **L'intégrité :** Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
- **La confidentialité :** Seules les personnes autorisées ont accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.
- **La disponibilité :** Le système doit fonctionner sans faille durant les plages d'utilisation prévues, garantir l'accès aux services et ressources installées avec le temps de réponse attendu.

D'autres aspects concernant les utilisateurs sont aussi considérés comme des objectifs de la sécurité des systèmes l'information. Ces aspects sont des fois rassemblés sous le nom d'**Auditabilité de l'information** :

- **La non-répudiation** (**l'imputation**) : 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.
- **La traçabilité** (**Preuve**) : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservables 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. Elle consiste à s'assurer de la certitude de l'identité d'une personne (*Authentification = Identification + Certitude*).

## *IV. Les causes de l'insécurité (classification de menaces) :*

Les causes de l'insécurité sont de divers aspects :

- Ils peuvent avoir un rapport direct avec l'informatiques ou bien aucun lien avec.
- Ils peuvent être suite à une action intentionnelle (malveillante) ou bien à une action pas malveillante (un accident, une faute, ou un évènement naturel).
- Ils peuvent provenir d'une source de l'intérieur du système ou bien de son extérieur.
- La majorité des causes sont suite à une action humaine, mais d'autres non.

### *a. Causes humaines :*

- **La maladresse :** Quelqu'un peut exécuter un traitement non souhaité, effacer involontairement des données ou des programmes.

- **L'inconscience :** de nombreux utilisateurs méconnaissent les risques, et introduisent souvent des programmes malveillants sans le savoir, ou effectuent des manipulations inconsidérées.
- **La malveillance** : une personne parvient à s'introduire sur le système, légitimement ou non, et à accéder ensuite à des données ou à des programmes.

La majeure partie des menaces est due à l'erreur ou la négligence humaine (utilisateurs comme informaticiens). Il ne faut pas les ignorer ou les minimiser.

### b. Causes extérieures

- Un sinistre (vol, incendie, dégât des eaux).
- Une **malveillance** ou une mauvaise manipulation entraînant une perte de matériel et/ou de données.
- **Problèmes électriques**. L'alimentation électrique n'est pas à négliger.

### c. Causes techniques

- Surchauffe : les processeurs produisent de la chaleur.
- **L'usure :** elle est inévitable. En tenir compte donc !
- Incidents liés au logiciel : des failles permettant de prendre le contrôle total ou partiel d'un ordinateur.
- Un **programme malveillant** : un logiciel destiné à nuire au système.

## V. Processus de sécurisation

Comme nous l'avons déjà cité la sécurité informatique est un processus en perpétuelle évolution. Ce processus permet de faire évoluer le système d'information que ce soit au niveau des choix technologiques ou au niveau de l'organisation des ressources utilisées pour assurer son fonctionnement.

En général, la sécurisation du système s'appuie sur le principe de la roue de ***Deming*** ou la méthode ***PDCA*** (***Plan-Do-Check-Act***) pour instaurer une méthode de management de risques informatiques au sein d'un organisme. Ce principe permet de définir la démarche suivie pour l'implémentation d'une politique de sécurité efficace et l'inscrire dans un contexte d'amélioration continue afin de garantir une évolution sereine et maîtrisée d'un système d'information donné.


**Figure 1 : Démarche de sécurisation d'un système**

- L'implémentation d'un tel processus passe tout d'abord par la définition de la politique de sécurité informatique afin d'identifier les risques et élaborer les objectifs de sécurité (Plan).
- Ensuite il faut mettre en place les mesures sécuritaires définies pour atteindre les objectifs fixés par la PSSI (Do).
- Après il faut vérifier que ces mesures couvrent l'essentiel de la chaîne sécuritaire du système d'information sachant que la sécurité de ce dernier est comparée à celle de son maillon le plus faible (Check).
- Enfin analyser les résultats, réagir selon le niveau de sécurité obtenu, identifier les ressources qui nécessitent des modifications et bien entendu suivre l'évolution des nouvelles menaces et les traduire en mesures sécuritaires dans la PSSI (Act).

De plus la majorité des méthodes d'analyse de la sécurité des systèmes d'information visent la mise en place d'un système de management de la sécurité informatique (SMSI) au sein des organismes. En effet, ces méthodes reprennent les grandes lignes du PDCA pour formaliser un SMSI pour ensuite aller plus dans le détail afin de garantir une gouvernance rationnelle de la sécurité informatique au sein des entreprises.

## *Références :*


- L. Bloch & C. Wolfhugel "Sécurité informatique : Principes et méthodes à l'usage des DSI, RSSI et administrateurs" Eyrolles 2ème édition 2013.
- S. Ghernaouti « Cybersécurité Analyser les risques Mettre en œuvre les solutions » DUNOD 6ème édition 2019.
- COMPUTER SECURITY RESOURCE CENTER https://csrc.nist.gov/
- La défense en profondeur appliquée aux systèmes d'information https://www.ssi.gouv.fr/ Version 1.1 – 19 juillet 2004
- Sécurité des systèmes d'information https://fr.wikipedia.org/
- PDCA : savoir utiliser la roue de Deming https://www.techniques-ingenieur.fr/