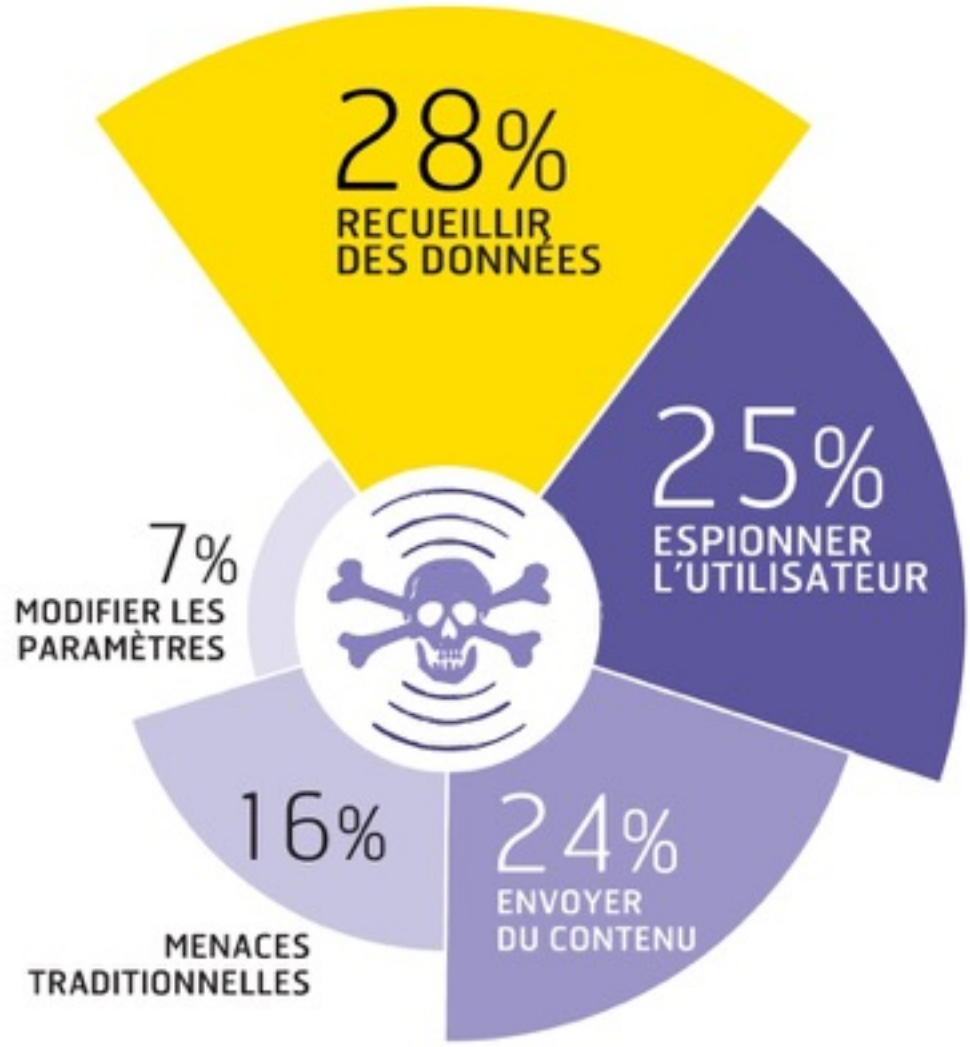
SÉCURITÉ INFORMATIQUE: L'ESSENTIEL



SOURCE : DOCUMENTS FOURNIS PAR NOËL MACÉ, DOMINIQUE MOUCHENÉ ET PIERRE-FRANÇOIS BONNEFOI; IMAGE DE FRANCOIS MARET, LES ECHOS; ICÔNES DE FLATICON.

GÉNÉRALITÉS SUR LA SÉCURITÉ

Qui n’a jamais perdu de fichiers informatiques ou enregistré des données sur un support amovible (clé usb, ordinateur portable, smartphone, ...) qu'il a perdu?

Dans ce chapitre sur la sécurité informatique, nous ferons un rapide tour d’horizon de la sécurité des systèmes d'information. Il n'est ni totalement exhaustif, ni vraiment complet, et n'a pour but que de vous donner un aperçu des enjeux de la sécurité informatique.

Après une rapide introduction du vocabulaire et des notions fondamentales, la présentation se compose en trois parties: sécurité offensive, opérationnelle et défensive

Pré-requis : notions fondamentales d'informatique (réseau, systèmes d'exploitation, langages, etc.)

Définition

La sécurité, au sens général, consiste à se "protéger". Il existe de nombreux des domaine d'application de la sécurité: sécurité des personnes, sécurité nationale, internationale ou civile, économique, alimentaire, etc. Tous ont ce point commun le "sentiment de sécurité", par définition subjectif, et donc jamais absolue.

Sécuriser un système, c'est avant tout définir un "cadre d'utilisation", c'est à dire définir ce qui pourra (devra) ou ne pourra pas être fais, et mettre en place les éléments pour appliquer cette politique.

"La sécurité informatique consiste ainsi à garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu"
JF Pillou

Limites

Liberté

Quelque soit le domaine d'application, la sécurité est toujours à opposer à la liberté. En effet, la politique de sécurité établi les comportements acceptables ou non pour prémunir du danger, et définie donc des comportements "interdits". Cependant, un responsable en sécurité doit garder à l'esprit les libertés de l'usager, et éviter tout comportement excessif, souvent perçu comme une entrave abusive.

Acceptation

Conséquence direct du point précédent, une politique de sécurité se doit d'être comprise et acceptée. Sans cela, tout usager peu alors sortir des comportements prévus, volontairement ou non, et ainsi compromettre la sécurité du système.

Sécurité des systèmes d'information (SSI)

La SSI consiste surtout à protéger les informations manipulées, c'est à dire de l'information et ses outils d’accès.

Domaines d'application

Sécurité offensive

La sécurité offensive, comme son nom l'indique, consiste à "attaquer". Même si de nombreuses personnes apprennent ces méthodes (généralement de manière autodidacte) dans un but peu louable, ces techniques sont également enseignée soit dans le cadre de l'ethical hacking, permettant de déterminer les failles d'un système de manière légale, soit dans le cadre d'un audit préalable indispensable à la sécurité défensive ("connaitre ses ennemis pour mieux se défendre").

Sécurité défensive

Là où il y a des risques, il doit nécessairement y avoir une protection face à ces risques. La sécurité défensive se doit donc d'évaluer et quantifier les risques éventuels, de déterminer les failles à leur origine, et de déterminer en conséquence une politique de sécurité permettant de garantir la bonne marche (continuité) des affaires courantes.

Sécurité opérationnelle (OPSEC)

La sécurité opérationnelle consiste à la mise en œuvre de techniques, comportement et méthode permettant la protection des informations privées. Un très bon exemple de contexte dans lequel la sécurité opérationnelle est primordiale est le journalisme, particulièrement dans le cadre de la protection des sources.

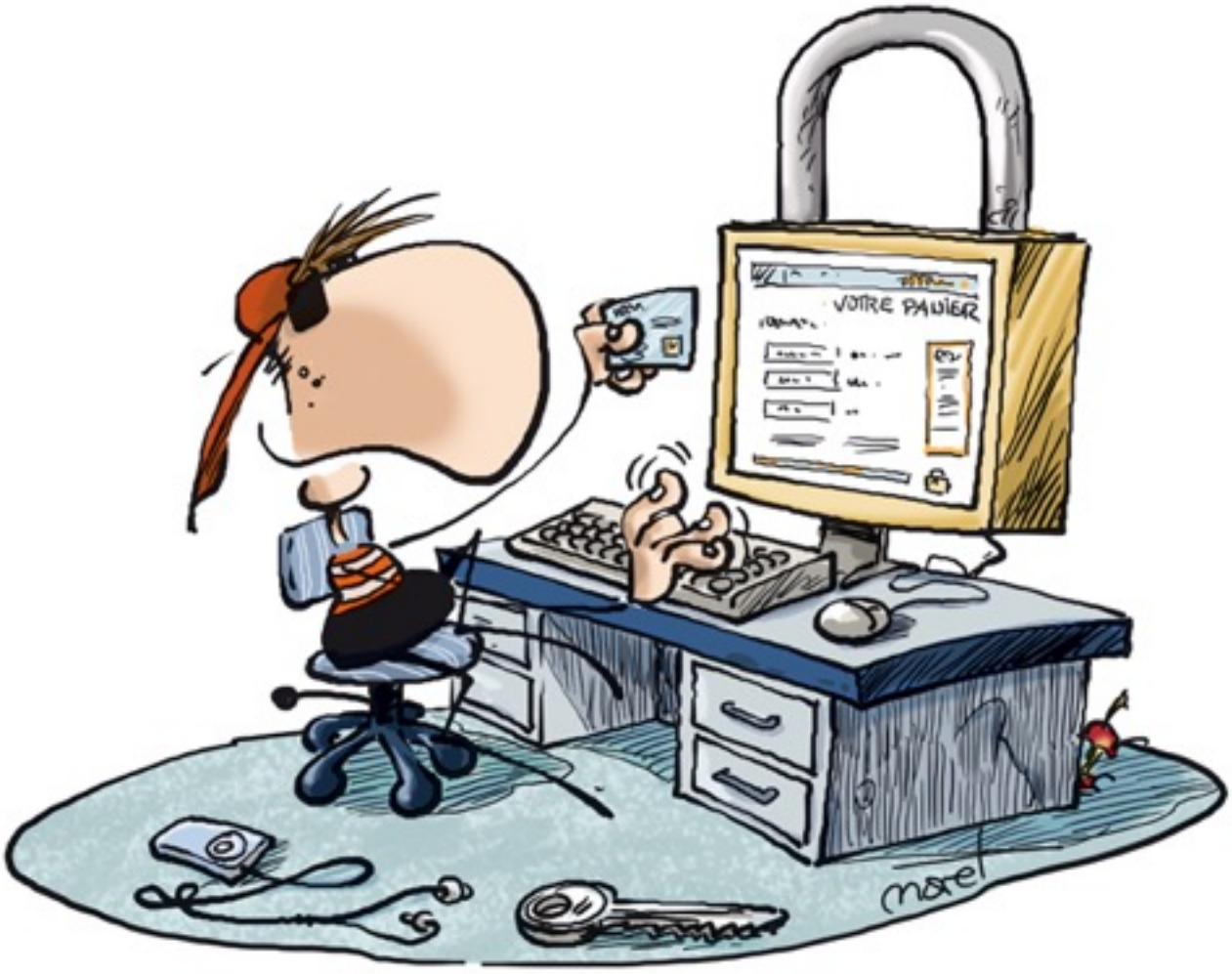
ENJEUX

Les enjeux de la SSI consiste en 3 points essentiels :

- **Intégrité**, garantie que l'information/donnée est bien celle attendu, et n'a donc pas été modifiée, de manière fortuite ou intentionnelle.
- **Confidentiel**, fait de réserver des informations à un nombre restreint de personnes (voir aussi OPSEC ci-dessus).
- **Disponible**, garantie du bon fonctionnement et du temps de réponse d'un système / service

A ces 3 points essentiels doivent être ajoutés deux points complémentaires, le plus souvent simples outils pour la réalisation des points précédents, mais parfois considérés comme des buts en soit (essentiellement pour des questions juridiques):

- **non-répudiation**, garantie qu'un utilisateur ne puisse contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et imputation, garantie qu'un aucun tiers ne puisse s'attribuer les actions d'un autre utilisateur.
- **L'authentification** est donc bien entendu un préalable indispensable à la confidentialité, l'imputation et la non-répudiation.



DÉMARCHE

Mettre en place une politique de sécurité se réalise en 3 étapes :

1. Evaluation des risques
2. Recherche et choix de parades
3. Mise en œuvre des protections

Elle répond aux questions suivantes:

- Aperçu des coûts d'incidents informatiques déjà survenus
- Qu'est-ce que les clients et les utilisateurs espèrent de la sécurité ?
- Quels sont les services prioritaires et ressources (locaux, équipement, personne) disponibles? Y a-t-il des services accessibles de l'extérieur?
- Quelle est la durée maximale d'interruption admissible (Recovery Time Objective) ?
- Quelles sont les règles juridiques applicables à l'entreprise concernant la sécurité et la confidentialité des informations (archives comptables ou protection de la sphère privée, voir plus loin les lois applicables en Suisse)?

Risques

Par risque, on entend les risques

- **Socio-géographiques**, comme l'atteinte à la vie privée, la divulgation de sources, d'informations de localisation ou accès, d'informations médicales, fiscales, etc.
- **Financiers**, direct, nécessitant la reconstituation / réparation des données et outils compromis ou indirectes comme l'indisponibilité d'un outil clé (comme un service de gestion de commande) suite par exemple à des attaques de spams, virus, panne électrique ou dégât d'eau.
- **D'image**, là également, directe, par la divulgation d'une faille de sécurité, supposant d'un manque de fiabilité ou indirecte (perte de confiance, désinformation, etc.) faisant suite par exemple à l'existence de chevaux de Troie ou autres logiciels espions (spywares) souvent inclus dans des logiciels P2P (peer to peer) ou multimédia.

Aujourd'hui l'hameçonnage (phishing), courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles et le canular informatique (hoax), courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes sont des pratiques très répandues dans le monde des affaires.

Parades

La recherche et le choix de parades consiste à déterminer, en fonction des risques évalués, les parades adéquates. Cela passe bien entendu par une évaluation des coûts et moyens. Se prémunir d'un risque par une solution dont la mise en place devrait avoir un coût supérieur que le risque lui même est peut être inutile!

Mise en œuvre des protections

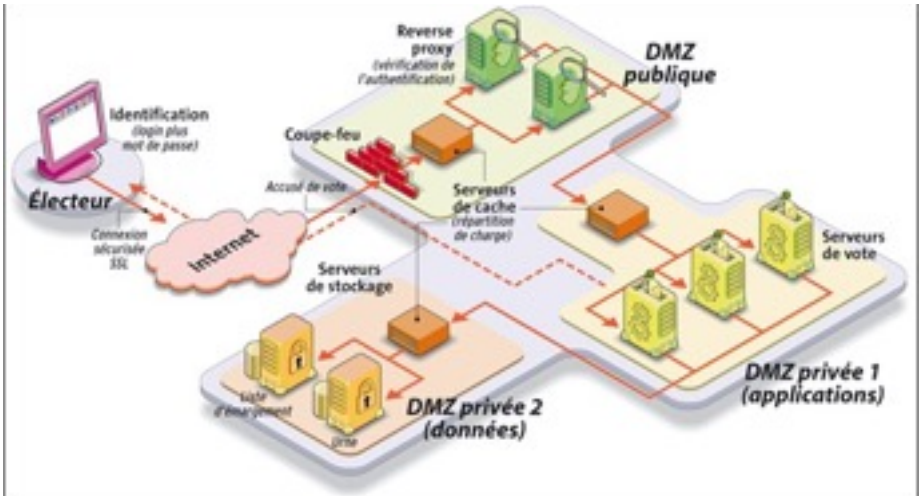
Suivant directement la phase d'analyse, la mise en œuvre se doit d'être perpétuellement testée. Elle peut également nécessiter de reprendre une analyse sur quelques points particuliers, sans devoir cependant remettre totalement en cause les conclusions de l'analyse préalables.

A noter que bien souvent les utilisateurs, eux-mêmes, sont à l'origine de pertes de données : par malveillance ou par maladresse. Documents non enregistrés, effacés ou perdus lors de manipulations hasardeuses sont source d'importantes pertes de temps et d'animosité à l'égard de l'outil informatique.
La protection contre ce risque passe par une connaissance de base du fonctionnement d'un ordinateur et, en particulier, du système de fichiers (notions d'arborescence, dossier, fichier...). Des habitudes efficaces et bien maîtrisées de création et d'enregistrement des documents sont indispensables: création des documents directement dans un dossier adapté, enregistrement à intervalles réguliers pendant le travail, maîtrise des opérations de copier/couper/coller limitent les risques de fausse manœuvre.

Précautions

Dans le cas des risques matériels il est possible de se prémunir grâce à de
La redondance informatique, en doublant ou en triplant un équipement (par des techniques de RAID ou de virtualisation), on divise le risque total par la probabilité de pannes simultanées.
La dispersion des sites, un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.
Des procédures de contrôle indépendants qui permettent bien souvent de déceler les anomalies avant qu'elles ne produisent des effets dévastateurs.

Enfin, malgré toutes les précautions prises contre les risques évoqués plus haut, il peut arriver que des données soient perdues; le temps mis à les créer, la complexité de leur élaboration, leur caractère vital sont autant de facteurs aggravants de cette perte. C'est pourquoi le recours à des procédures de sauvegarde (backup) est indispensable, au moins pour les données essentielles: il s'agit de conserver, en lieu sûr, une copie de ces données.



EXEMPLE D'ARCHITECTURE SÉCURISÉE: VOTE ÉLECTRONIQUE.

LOIS APPLICABLES[1]

- **Constitution fédérale (Cst ; RS 101)**
  art. 13 : protection de la sphère privée, notamment des correspondances postales [s'applique aux e-mails privés des employés]
- **Code civil (CC ; RS 210)**
  art. 27 ss : protection de la personnalité [comprend la protection de la sphère privée]
- **Code des obligations (CO ; RS 220)**
  art. 14 al. 2bis: validité de la signature qualifiée selon la Loi sur la signature électronique
  art. 59a : responsabilité de prendre des mesures de sécurité pour éviter une utilisation abusive de la clé de signature ; standard minimum défini à l'art. 11 de l'Ordonnance sur la signature électronique
  art. 332 : droit sur des inventions et des designs développés par les employés
  art. 728a : système de contrôle interne
  art. 957 ss. : obligation de tenir et de conserver les livres (ce qui comprend la correspondance commerciale), concrétisée par l'Ordonnance concernant la tenue et la conservation des livres de compte (Olico ; RS 221.431)
- **Loi sur le droit d'auteur et les droits voisins (Loi sur le droit d'auteur, LDA, RS 231.1)**
- **Loi sur les brevets d'invention (LBI ; RS 232.14)**
- **Loi fédérale sur la protection des données (LPD ; RS 235.1) et Ordonnance relative à la loi fédérale sur la protection des données (OLPD ; RS 235.11)**
- **Loi fédérale contre la concurrence déloyale (LCD, RS 241) [notamment interdiction de Spam, art. 3 lit. o LCD]**
- **Code de procédure civile (CPC ; RS 272)**
  art. 177 : admissibilité de fichiers électroniques comme preuve par titres
- **Code pénal (CP ; RS 311.0)** [Pour l'essentiel, il s'agit de se prémunir contre des actes punissables commis par les employés, p.ex. téléchargement d'images de pornographie dure]
  art. 135 : Interdiction de représentations d'actes violents par des moyens électroniques
  art. 143 : Soustraction de données
  art. 143bis : Accès indu à un système informatique
  art. 144bis : Détérioration de données
  art. 147 : Utilisation frauduleuse d'un ordinateur
  art. 197 : Interdiction de pornographie
  art. 251 : Faux dans les titres
- **Loi sur le travail dans l'industrie, l'artisanat et le commerce (LTr ; RS 822.11)** avec l'Ordonnance 3 relative à la loi sur le travail (Hygiène) (OLT 3 ; RS 822.113)
  art. 26 OLT 3 : Interdiction de l'utilisation de systèmes de surveillance destinés à surveiller le comportement des employés [prohibe notamment la surveillance automatique et non- anonymisée des e-mails et des accès Internet par les employés]
- **Loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique ; SCSE ; RS 943.03) et Ordonnance sur les services de certification dans le domaine de la signature électronique (Ordonnance sur la signature électronique, OSCSE)**

---

[1] http://www.hesge.ch/heg/sites/default/files/ccsie/documents/ressources-cadre-juridique-pme.pdf

PROTECTION DES DONNÉES PERSONNELLES

7 principes clés de la protection des données personnelles[2]

Le principe de finalité

Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage déterminé et légitime, correspondant aux missions de l'établissement, responsable du traitement. Tout détournement de finalité est passible de sanctions pénales.

Le principe de proportionnalité

Seules doivent être enregistrées les informations pertinentes et nécessaires pour leur finalité.

Le principe de pertinence des données

Les données personnelles doivent être adéquates, pertinentes au regard des objectifs poursuivis.

Le principe de durée limitée de conservation des données

C'est ce que l'on appelle le droit à l'oubli. Les informations ne peuvent être conservées de façon indéfinie dans les fichiers informatiques. Une durée de conservation doit être établie en fonction de la finalité de chaque fichier. Au-delà, les données peuvent être archivées, sur un support distinct.

Le principe de sécurité et de confidentialité

Le responsable du traitement, est astreint à une obligation de sécurité. Il doit faire prendre les mesures nécessaires pour garantir la confidentialité des données et éviter leur divulgation: le responsable du traitement doit prendre toutes mesures pour empêcher que les données soient déformées, endommagées ou que des tiers non autorisés y aient accès et des mesures de sécurité, tant physique que logique, doivent être prises (comme protection anti-incendie, sauvegarde, installation de logiciel antivirus, changement fréquent des mots de passe, etc.)

Le principe de transparence

La loi garantit aux personnes l'information nécessaire relative aux traitements auxquels sont soumises des données les concernant et les assure de la possibilité d'un contrôle personnel. Le responsable du traitement de données personnelles doit avertir ces personnes dès la collecte des données et en cas de transmission de ces données à des tiers.

Le principe du respect du droit des personnes

- Obligation d'informer les intéressés
- Droits d'accès et de rectification
- Droit d'opposition

[2] source: cnrs