Les 3 principaux objectifs à ne pas perdre de vue

1. **Confidentialité**
2. **Intégrité**
3. **Disponibilité**

!!! ATTENTION AU MAILLON LE PLUS FAIBLE !!!

1. Confidentialité

- A échange un message avec B.
- A et B doivent rester les seuls à connaitre le contenu du message.
- Idem pour une donnée stockée dans un système.

<u>Le danger:</u>

Un accès (accidentel ou intentionnel) non désiré au contenu de l'information stockée ou échangée.

2. Intégrité

- A échange un message avec B
- Le message reçu par B doit être tel que A l’a envoyé (non modifié).
- Idem pour une donnée stockée dans un système.

Le danger:

Une modification (altération accidentelle ou intentionnelle) non désirée de l'information stockée ou échangée.

3. Disponibilité

- Les systèmes informatiques utilisés doivent toujours rester opérationnels pour permettre un accès constant à la ressource souhaitée (service ou donnée).

<u>Le danger:</u>

La non disponibilité accidentelle (ex: panne) ou intentionnelle (due à une malveillance).

Les autres objectifs importants

Les 3 A (**AAA)**:

4. **A**uthentication → authentification (de l'identité),
5. **A**uthorization → autorisation,
6. **A**ccounting →journalisation/auditabilité/imputabilité

Mais aussi:

7. Authenticity → **authenticité**, authentification (de quelque chose),
8. Nonrepudiation → **Irrévocabilité**.

4. Authentification (au sens AAA)

- A et B doivent disposer d'un moyen technique de prouver qu'ils sont bien les personnes qu'ils prétendent être.
- Il en va de même pour les services informatiques utilisés par A et B (ex: un serveur web est-il celui qu'il prétend être ?).

<u>Le danger:</u>

L'usurpation d'identité.

Authentification/Identification

- Identification = répondre à la question « qui êtes vous ? » ou « qui est-ce ? ».

Par exemple, en fournissant son nom d'utilisateur.

- Authentification = en apporter la **preuve** = prouver le caractère authentique de l'identité (*).

Par exemple, en fournissant son mot-de-passe.

(*) « *Caractère permanent et fondamental de quelqu'un, d'un groupe, qui fait son individualité, sa singularité.* » (Déf. Larousse)

!!! Beaucoup d'ambiguïtés possibles !!!

La preuve

- Quelque chose que je sais,
- Quelque chose que je possède,
- Quelque chose que je suis (= prouver son identité par son identité…!!!)
- + éventuellement la localisation.

Caractéristique à garder en tête:

Une bonne preuve doit pouvoir être facilement révoquée (*) en cas de compromission.

(*) à interpréter comme « supprimée/modifiée ».

Ex. d’ambiguïtés possibles:

Jeu: « identifie ou authentifie ? »

- La carte d’identité,
- L’empreinte digitale,
- Une signature,
- …

5. Autorisation

- A, B et C accèdent à un fichier:
  - A peut le lire, le modifier et le supprimer,
  - B peut le lire et le modifier,
  - C peut uniquement le lire.

Le danger:

L'accès non autorisé à une ressource (fichier, service) ou l'accès avec de mauvaises autorisations (droits).

Rem.
Pour que ce système fonctionne, le SI doit être en mesure de savoir s'il a affaire à A, B ou C → qui est qui + idéalement en apporter la preuve = l'authentification.

→ Les objectifs de sécurité ne sont pas toujours dissociables.

6. Accounting [pas facile à traduire 😒 …]

- A et B utilisent les ressources du SI.
- Le système doit fournir un outil permettant de dire qui fait quoi ou qui a fait quoi.

<u>Le danger:</u>

L'incapacité de déterminer qui utilise les ressources du SI et comment ces intervenants l'utilise.

<u>Rem.</u>

! au lien étroit existant entre cet objectif et la loi… puis-je « tracker » mes utilisateurs ?

7. Authenticité (de quelque chose)

- A doit envoyer un message à B.
- Le message reçu par B doit être tel que transmis par A (intègre).
- Mais en plus, B doit disposer d'une preuve lui permettant d'affirmer que le message vient bien de A (authentifié).

Rem.

Certains objectifs peuvent donc se combiner pour en former de plus complets.

8. Non-répudiation (Irrévocabilité)

- Il s’agit d’empêcher une entité (personne, entreprise) de nier une action accomplie.
- A achète sur le web un objet à B.
- A ne peut pas nier avoir accompli cet achat (et doit donc payer B).
- De même si A a bien payé B, alors ce dernier ne peut pas prétendre ne pas avoir reçu l’argent.

<u>Le danger:</u>

Nier volontairement des actions accomplies ou des engagements pris.

Comment en savoir plus / Qui fait quoi ?

Les organismes publics orientés cybersécurité

- CCB: https://www.ccb.belgium.be/
- Safeonweb: https://www.safeonweb.be/
- ANSSI France: https://cyber.gouv.fr/
- Cyberwal (Digital Wallonia) : https://www.digitalwallonia.be/fr/programmes/cyberwal-by-digital-wallonia/
- NIST USA : https://www.nist.gov/
- ENISA EU: https://www.enisa.europa.eu/media/enisa-en-francais/

Comment en savoir plus / Qui fait quoi ?

Les organismes publics orientés Protection DAC (RGPD/GDPR)

DACP: Données A Caractère Personnel

- APD: https://www.autoriteprotectiondonnees.be
- CNIL France: https://www.cnil.fr/

Comment en savoir plus / Qui fait quoi ?

D’autres organismes publics:

- La défense: https://www.mil.be/ (cf. SGRS ci-dessous)
- La police (FCCU et RCCU): https://www.police.be/5998/fr/a-propos/directions-centrales/federal-computer-crime-unit
- Les services de renseignement:
  - La sûreté de l’état: https://www.vsse.be/fr
  - Le Service Général du Renseignement et de la Sécurité (SGRS): https://www.vsse.be/fr/le-service-general-du-renseignement-et-de-la-securite-sgrs

Comment en savoir plus / Qui fait quoi ?

Les CERTs

- CERT belge: https://www.cert.be/
- CERT français: https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/
- CERT luxembourgeois: https://www.govcert.lu
- CIRCL Luxembourg: https://www.circl.lu/
- CERT USA: https://us-cert.cisa.gov/

Comment en savoir plus / Qui fait quoi ?

Les initiatives entre secteur privé et secteur public

- Cyber Security Coalition: https://www.cybersecuritycoalition.be

Comment en savoir plus / Qui fait quoi ?

Le monde de la formation

- Système scolaire « conventionnel »: écoles, H-E, universités
- Organismes subventionnés (p.ex. centres de compétence)
- Acteurs privés spécialisés dans la formation
- Industriels proposant leur(s) propre(s) cursus et/ou certification

Titres remis possibles:

Diplôme, certificat, certification, attestation de suivi,…

Comment en savoir plus / Qui fait quoi ?

Les monde des certifications

- CEH
- CISSP
- OSCP
- Cisco
- ISO 27001 lead implementer
- …

Comment en savoir plus / Qui fait quoi ?

La documentation spécialisée

- Orientée web: blogs, sites, podcasts…
- Orientée livre: maisons d'édition conventionnelles ou spécialisées.
- Orientée magazine: presse spécialisée.

Quelques exemples:

- https://www.nolimitsecu.fr/
- https://www.deboecksuperieur.com/ouvrage/9782807321885-hacking-et-contre-hacking 😉
- MISC magazine: https://connect.ed-diamond.com/MISC