Introduction à la sécurité

Module 2

Introduction à la sécurité des systèmes d'informations

Pablo Rauzy <pr@up8.edu>
pablo.rauzy.name/teaching/is

Introduction à la sécurité des systèmes d'informations

La sécurité des systèmes d'informations

- Jusqu'à présent on a étudié la cryptologie :
  - elle permet de protéger des secrets et de communiquer de manière sécurisée,
  - c'est essentiellement un outils au service de la sécurité,
  - mais elle ne permet pas de régler tous les problèmes de sécurité.
- Dans ce nouveau module du cours, on va s'intéresser à la sécurité des systèmes au delà de la cryptologie.

Un domaine plus large que l'informatique

- La sécurité d'un système d'information nécessite une gestion bien plus large que simplement celle des informaticien·nes.
- En amont, il est nécessaire d'identifier les risques et d'évaluer leur importance.
  - Cela doit être fait en partenariat avec les expert·es métiers et les décideur·es.
  - Il s'agit parfois de décisions plus politiques que techniques.
- En aval, il est nécessaire d'établir des plans de reprises d'activité.
  - À nouveau, cela ne peut être le seul fait des experts en sécurité.
- Entre les deux, les mesures de sécurité ne peuvent être uniquement techniques.

Un domaine plus large que l'informatique

- La sécurité d'un système d'information nécessite une gestion bien plus large que simplement celle des informaticien·nes.
- En amont, il est nécessaire d'identifier les risques et d'évaluer leur importance.
  - Cela doit être fait en partenariat avec les expert·es métiers et les décideur·es.
  - Il s'agit parfois de décisions plus politiques que techniques.
- En aval, il est nécessaire d'établir des plans de reprises d'activité.
  - À nouveau, cela ne peut être le seul fait des experts en sécurité.
- Entre les deux, les mesures de sécurité ne peuvent être uniquement techniques.
  - Notamment parce que les humains sont la première vulnérabilité exploitée.

Les aspects techniques

- Quelles mesures de sécurité connaissez-vous ? Que permettent-elles ? Que nécessite leur mise en œuvre ?

Les aspects techniques

- Quelles mesures de sécurité connaissez-vous ? Que permettent-elles ? Que nécessite leur mise en œuvre ?
- Quelques exemples :
  - Contrôle d'accès ou d'usage (mot de passe / certificat cryptographique).
  - Séparation des rôles et privilèges.
  - Analyse des logiciels contre les bugs et vulnérabilités (audit / méthodes formelles).
  - Pare-feu et surveillance du réseau.
  - Logiciels anti-virus et anti-spam.
  - Chiffrement, signature, etc.

Contenu du module

- L'objectif de ce cours est de vous faire prendre conscience de l'importance de la sécurité.
- C'est plus fun et plus mémorable d'aborder tout ça côté attaquant·e.

- J'appelle la sécurité système celle des logiciels (OS comme applications).
- Elle concerne par exemple :
  - les portes dérobées,
  - les chevaux de Troie,
  - les rootkits,
  - les dépassements de mémoire tampon,
  - etc.

- J'appelle la sécurité réseau celle qui concerne les attaques à distances, au travers d'un réseau (internet le plus souvent).
- On peut penser aux types d'attaques suivants:
  - écoute / capture de trafic réseau, scan de ports
  - attaques de l'intercepteur,
  - virus / vers,
  - empoisonnement ARP ou usurpation DNS,
  - déni de service,
  - etc.

- J'appelle la sécurité web celle qui s'occupe des vulnérabilités spécifiques aux applications web, de plus en plus répandues.
  - injections SQL,
  - XSS (cross-site scripting),
  - CSRF (cross-site request forgery),
  - etc.

- L'ingénierie sociale est la partie de la sécurité qui s'attaque aux vulnérabilités des humain·es, dont la sécurité est la plus difficile à garantir.
  - clef USB,
  - phishing,
  - usurpation au téléphone,
  - pénétration de bâtiment IRL,
  - etc.