

# Sécurité informatique

## Modèle de menaces

En matière de sécurité informatique, l'analyse des risques consiste à *calculer la probabilité que les menaces puissent réussir*, de sorte que vous savez *combien d'efforts à dépenser pour défendre contre eux*.

Il peut y avoir de nombreuses façons différentes que vous pourriez perdre le contrôle ou l'accès à vos données, mais certains d'entre eux sont moins susceptibles que d'autres. **Évaluer le risque signifie décider quelles menaces vous allez prendre au sérieux** et qui peuvent être trop rares ou trop inoffensives (ou trop difficiles à combattre) à s'inquiéter.<sup>1)</sup>

L'analyse peut se faire sur une base régulière pour tenir compte de nouveau facteurs. Une première étape concrète est la **modélisation des menaces**.

## Cinq questions pour évaluer votre modèle de menace

- Que souhaitez-vous protéger ?
- Contre qui souhaitez-vous le protéger ?
- Quelle est la probabilité que vous ayez besoin de le protéger ?
- Quelles seraient les conséquences si vous échouiez ?
- Quels désagréments êtes-vous disposé à affronter afin de vous en prémunir ?

## Quelques conseils

- Écrivez une liste de données que vous rangez, où vous la rangez, qui y a accès et les mécanismes qui évitent que les autres y aient accès.
- Faites une liste de ceux qui seraient susceptibles de souhaiter s'approprier de vos données ou communications. Il peut s'agir d'une personne, une agence du gouvernement ou une corporation.
- Écrivez ce que votre adversaire est susceptible de vouloir faire avec vos données privées.

## Un exemple

- Est-ce que je dois fermer la porte de mon bureau? À clé?
- Quel type de serrure ou de verrous devrais-je investir?
- Ai-je besoin d'un système de sécurité plus avancé?
- Quels sont les biens à protéger dans ce scénario?
  - Des documents physiques avec des données sensibles
  - Des biens de valeur (électronique, vêtements, équipement de bureau)

- Des articles sans valeur
- Quelle est la menace?
- \* Quelqu'un pourrait entrer par effraction.
- \* Quelqu'un pourrait profiter d'une opportunité de vol rapide
- Quel est le risque réel d'effraction? Quelle en est la probabilité?

Une fois que vous vous êtes posé ces questions, vous êtes en mesure d'évaluer les mesures à prendre:

- Si vos biens sont précieux, mais le risque d'un effraction est faible, alors vous ne voudrez probablement pas investir trop d'argent dans une serrure.
- S'il y a conséquence grave d'avoir des données ou documents sensibles exposés (congédier? danger physique?), votre organisation sera probablement responsable de mettre en place de plus fortes mesures de sécurité
- D'autre part, si le risque est élevé, vous voudrez obtenir les meilleurs verrous sur le marché, et peut-être même ajouter un système de sécurité.

## Liens utiles

\* [https://en.wikipedia.org/wiki/Threat\\_model](https://en.wikipedia.org/wiki/Threat_model) \*

[https://en.wikipedia.org/wiki/DREAD\\_\(risk\\_assessment\\_model\)](https://en.wikipedia.org/wiki/DREAD_(risk_assessment_model))

## Références

\* [Une Introduction au Modèle de Menace, EFF](#)

<sup>1)</sup>

<https://ssd.eff.org/en/glossary/risk-analysis>

From:

<https://dulib.re/wiki/> - Le Goût du Libre

Permanent link:

[https://dulib.re/wiki/doku.php/securiteinformatique\\_modelemenaces?rev=1486125973](https://dulib.re/wiki/doku.php/securiteinformatique_modelemenaces?rev=1486125973)

Last update: **2017/02/03 04:46**

