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 sachiez *combien d'efforts à dépenser pour vous défendre contre ces menaces*.

Il peut y avoir de nombreuses façons différentes dont vous pourriez perdre le contrôle ou l'accès à vos données, mais certaines d'entre elles sont moins susceptibles que d'autres. **Évaluer le risque signifie décider quelles menaces vous allez prendre au sérieux** et lesquelles peuvent être trop rares ou trop inoffensives (ou trop difficiles à combattre) pour s'en inquiéter. [1)]

L'analyse peut se faire sur une base régulière pour tenir compte de nouveaux 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.
- Faîtes 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 (congédiement? 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/DREAD_(risk_assessment_model)

Références

* Une Introduction au Modèle de Menace, EFF

[1)]
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=1565178608

Last update: **2019/08/07 04:50**