Règle n° 1 : identifier ses risques et son attractivité face aux cybercriminels

La cybercriminalité évolue à un rythme effréné, suivant une dynamique similaire à celle de l'utilisation des systèmes d'information. Cette criminalité revêt de multiples formes et comporte de nombreuses dimensions que les entreprises doivent comprendre et considérer en fonction de leurs activités.

Si Socrate préconisait de se connaitre soi-même, Sun-Tzu lui recommande de connaître ses ennemis. Afin de se prémunir des activités cybercriminelles qui peuvent nuire à l'entreprise, les bonnes pratiques sont :

- **Analyser a minima annuellement les évènements que vous redoutez et dont vous voulez vous prémunir.** Pour cela il faut identifier actifs de l'entreprise potentiellement attractifs pour les différentes catégories de cybercriminels. Même s'il est parfois difficile d'établir une limite claire entre les différentes motivations des cybercriminels, nous pouvons en distinguer 4 majeures :
  - **L'idéologie** qui s'attaque à l'image de marque de l'entreprise en frappant les sites web (indisponibilité ou modification malveillante) ou en volant et révélant sur Internet des données.
  - **Les gains financiers directs** obtenus via le vol de données bancaire, personnelles, ou de secrets stratégiques, ou encore par le paiement de rançon suite à une attaque bloquant le SI (ransomware).
  - **L'espionnage, la déstabilisation entre États ou le cyberterrorisme,** qui visent à détruire des systèmes critiques ou à voler des données stratégiques afin de nuire au bon fonctionnement des services critiques ou vitaux des États.
  - **La facilitation d'attaques** en ciblant de sous-traitants de grandes entreprises pour voler des données ou rebondir vers d'autres systèmes.
- **Communiquer sur les mesures prises en termes de cybersécurité auprès de ses actionnaires mais aussi auprès de ses clients présente plusieurs avantages cruciaux :**
  - Identifier les scénarios qui auront le plus d'impact sur l'actionnariat et sur la relation client, qui peuvent être différents des scénarios les plus impactants techniquement ou fonctionnellement.
  - Réduire le choc ressenti si une cyberattaque touche l'entreprise.

Il est surtout primordial de prendre conscience que de nos jours, **ces attaques peuvent toucher n'importe quelle entreprise, quel que soit son secteur d'activité**, comme l'a récemment montré l'actualité.

Faits / exemples d'impacts

Sony Picture (2014) : attaque idéologique menant à la destruction totale du système d'information (effacement de dizaine de millier de PC), ainsi qu'au vol et à la publication du patrimoine informationnel de l'entreprise.

Target (2013) : 40 millions de données bancaires et de plus de 70 millions de données personnelles volées chez ce spécialiste de la grande distribution. L'attaque avait ciblée initialement le fournisseur en charge de l'entretien du chauffage. L'attaque a couté 252 millions de dollars à Target et a rapporté au moins 2 millions de dollars aux attaquants.

Black Energy (2015) : piratage du réseau électrique ukrainien probablement liée à la situation géopolitique de ce pays. 250 000 foyers ont été plongés dans le noir pendant 3 à 6h.

Résultats attendus

Identification des 3 risques majeurs pour l'entreprise, soit :

- En fonction de ses actifs, des cybercriminels qui pourraient l'attaquer.
- En prenant en compte les mesures de sécurité déjà en place (organisationnelle et technique).

Les actions de maîtrise de ces risques à mettre en place, ainsi que les budgets associés et les responsables des chantiers

Développement d'un programme et des projets cybersécurité pour réduire et gérer les menaces cyber

Intégration de la cybersécurité dans les processus métiers et support de l'entreprise.