Évaluation des risques de cybersécurité pour les entreprises

Département de Communication et de Transformation Numérique

Une évaluation des risques en matière de cybersécurité vous aidera à comprendre à la fois vos processus commerciaux et les systèmes et données qu'il est important de sécuriser. La connaissance des risques peut vous aider à prévenir un incident de cybersécurité ou à vous en remettre.

1. Connaître vos systèmes et vos données

Assurez-vous de bien comprendre vos processus commerciaux et la façon dont vos systèmes et vos données s'y intègrent.

Documentez les systèmes et les données qui soutiennent vos processus commerciaux. Concentrez-vous sur les processus commerciaux qui sont les plus importants pour vous.

Cela signifie les systèmes qui sont essentiels au fonctionnement de votre entreprise, et les systèmes qui stockent vos données.

Vos systèmes seront:

- **interne** — ceux que vous accueillez, gérez et dont vous êtes responsable.
- **externe** — celles auxquelles vous accédez par un navigateur web, y compris celles gérées par une tierce partie.

Vos données comprendront:

- les données **personnelles** (comme les données des employés et des clientsi)
- données **financières**, et
- propriété **intellectuelle.**

Exemple

La comptabilité et la facturation constituent un processus commercial important. Si vous gérez cette activité dans votre propre entreprise, vous pouvez utiliser l'une ou l'autre:

- une application **interne**, comme Quickbooks, où les données sont stockées sur votre serveur sur place, ou
- une application **externe**, comme Xero, où les données sont stockées sur les serveurs de Xero.

Les données stockées par ces systèmes sont des données **financières** et **personnelles.**

2. Identifier les menaces et les vulnérabilités

Déterminez qui peut vouloir accéder à vos systèmes et données, et dans quelle mesure ils sont vulnérables ou exposés.

Pensez à ceux qui pourraient vouloir accéder à vos systèmes et à vos données, et aux **menaces** qui pèsent sur eux. Dans quelle mesure les systèmes sont-ils facilement accessibles et quelle est la valeur des données?

Ensuite, examinez dans quelle mesure les systèmes et les données sont **vulnérables** ou exposés. S'ils sont exposés à l'internet, ou s'ils ne nécessitent qu'une authentification de base pour y accéder, ils seront plus vulnérables aux attaques.

Envisagez d'engager un professionnel de la sécurité informatique pour vous aider à documenter les menaces et les vulnérabilités afin de vous assurer de ne rien manquer.

N'oubliez pas que toutes les menaces ne sont pas malveillantes. Une erreur commise par un employé peut aussi être une menace.

Exemple

Votre serveur web doit être accessible sur Internet pour héberger votre site web. La menace d'une attaque non ciblée contre lui est très probable, si:

- votre équipe informatique laisse un port d'accès à distance sur le serveur d'application exposé à l'internet, et
- il n'utilise qu'une authentification de base (nom d'utilisateur + mot de passe).

Un attaquant pourrait utiliser des outils automatisés pour deviner vos données de connexion et y accéder à votre insu.

3. Déterminer les risques ///

Lorsque vous avez identifié les menaces et les vulnérabilités, déterminez le risque que chacune d'entre elles présente.

Un risque est un événement causé par une menace et une vulnérabilité.
Il existe trois différents types de risques pour la sécurité. Il y a:

- **risques de confidentialité** — lorsque votre système ou vos données ne sont plus secrets.
- **risques d'intégrité** — lorsque votre système ou vos données ne sont plus exacts ou corrects.
- **risques de disponibilité** — lorsque vos systèmes ou vos données ne sont pas disponibles.

Le risque sera toujours un compromis. Certains risques doivent être acceptés, d'autres peuvent être gérés de manière à ce que le risque ne soit pas aussi élevé. L'identification de vos principaux risques est une première étape importante pour trouver la bonne stratégie de gestion.

Les risques pour la vie privée sont parfois pris en compte dans une évaluation des risques. La confidentialité des données personnelles, comme celle des données de vos clients, est un type de risque de confidentialité.

Exemple

Si un cyber-attaquant était en mesure d'accéder à votre courrier électronique, il pourrait l'utiliser pour:

- recueillir des informations commerciales sensibles, ce qui constitue un risque de **confidentialité**.
- enjoignez à vos clients d'effectuer les paiements sur leur compte bancaire plutôt que sur le vôtre, ce qui constitue un risque pour **l'intégrité**.

4. Définir les impacts ///

Documentez l'impact des risques - comment ils affecteraient votre entreprise s'ils se produisaient.

Catégoriser le type d'impact qu'aurait chaque risque.

- **Opérationnel** — comment le risque affecterait-il vos opérations quotidiennes?
- **Réputation** — que penseraient les gens de vous si le risque se concrétisait?
- **Financier** — combien coûterait le recouvrement de ce risque?
- **Technique** — comment le risque affecterait-il votre réseau ou votre environnement informatique?

Ensuite, attribuez à chacun une note d'impact faible, moyen ou élevé.

Cela vous aidera à définir une stratégie de gestion des risques et un plan pour les contrôler.

Exemple

- Si un agresseur avait accès aux données de messagerie de vos clients et les divulguait, cela aurait un impact important sur **la réputation** de votre entreprise.
- Si vous aviez une imprimerie et qu'un attaquant faisait tomber le serveur qui fait tourner le logiciel d'impression, cela aurait un impact **opérationnel** sur l'entreprise.

5. Mettre en œuvre les contrôles ///

Définissez les contrôles qui contribueront à prévenir ou à atténuer les risques de votre entreprise.

Décidez quels risques vous pouvez prendre :

- **contrôle**, en abaissant la cote de risque
- **transfert,** en faisant appel à un tiers pour les gérer à votre place
- **supprimer,** en fermant le système en péril, ou en ne collectant pas les données en péril
- **accepter,** si vous ne pouvez pas les supprimer entièrement.

En tant que propriétaire d'entreprise, les risques sont toujours de votre responsabilité - même si un tiers les gère pour vous.

Lorsque vous avez élaboré les contrôles à mettre en œuvre :

- mettez en place votre plan d'atténuation pour prévenir les risques
- parlez à votre personnel des risques auxquels l'entreprise est confrontée et de ce qu'ils peuvent faire pour assurer sa sécurité
- créer un plan de réaction aux incidents afin de savoir quoi faire en cas d'attaque.

Exemple

Si vous avez un système de paiement qui collecte des données personnelles de vos clients, vous pourriez le fermer et traiter les paiements par l'intermédiaire d'un tiers comme Paypal à la place.

Cela leur **transfère** le risque que les données soient compromises, sans que cela n'ait d'incidence sur votre entreprise ou vos clients.

Assurez-vous que votre personnel et les tiers avec lesquels vous travaillez comprennent également les risques et les contrôles de votre entreprise. Revoyez régulièrement votre évaluation des risques, car ceux-ci peuvent évoluer avec le temps.