

Les deux faces de la médaille: les risques de la cybersécurité et la gestion de la confiance avec des tiers

21 décembre 2021, 01:00

Tatiana Galibus

Chez Sirris, les experts en cybersécurité acquièrent aussi de l'expérience lors des coachings individuels en entreprise. Dans ce blog, nous partageons avec vous quelques-unes des nombreuses observations pratiques recueillies sur le terrain. Voici quelques conseils basés sur notre expérience en matière de sécurité le long de la chaîne logistique et sur la façon dont elle est traitée dans les entreprises.

Nous sommes souvent confrontés à des clients qui n'ont pas les connaissances ou l'expérience nécessaires pour gérer leurs interactions avec des tiers de manière sécurisée. En d'autres termes, les entreprises accordent souvent des droits d'administrateur aux fournisseurs de technologies dans leurs réseaux internes, ouvrent des ports à l'accès externe sans surveillance ni restrictions, etc. Il en résulte une menace directe pour des actifs essentiels et pour la continuité des activités.

Par ailleurs, nous coachons souvent des fournisseurs de technologies numériques dont les clients posent des questions sur le thème de la confiance, par exemple :

- Vos activités sont-elles sécurisées?
- Puis-je vous confier mes données en toute confiance?
- Quelles sont les garanties que votre service/produit numérique ne sera pas violé?

Nous constatons que le thème de la sécurité de la chaîne logistique gagne en importance et exige une attention accrue de la part des deux parties.

Vous externalisez des activités?

Vous courez un danger potentiel à chaque fois que vous donnez des droits d'accès à des services numériques, qu'il s'agisse d'une app, d'une plate-forme cloud, d'une application mobile, d'un SaaS, etc. Votre infrastructure interne, vos comptes, vos actifs, votre chaîne de production et vos données sensibles sont exposés au service externe de la même manière qu'à votre propre service interne. Mais pouvez-vous faire confiance à des tiers ? Comment vérifier la résilience du fournisseur de technologie avant de lui permettre d'accéder à votre réseau?

Dans la réalité, les interactions avec des tiers constituent une menace. Tout le monde a entendu parler de [l'attaque Solarwinds en décembre de l'année dernière](#). Les faits:

- Plus de 18 000 entreprises ont été touchées.

- Elle provenait d'un fournisseur de cybersécurité (le service Solarwinds), par l'intermédiaire d'une mise à jour de routine.
- De nombreuses entreprises ne savaient pas qu'elles avaient été victimes d'une attaque, car elles n'avaient pas de fichiers-journaux (logs).
- Même le ministère des Finances américain a été touché.

Au vu de ces preuves, peut-on faire aveuglément confiance à ses fournisseurs en matière de sécurité ? Et que faire en pratique ?

Notre conseil : la seule façon d'établir la confiance consiste à poser des questions. Vous pouvez faire appel à un auditeur externe (vous le payez et lui faites confiance pour contrôler les actifs les plus précieux de votre entreprise) mais, en parallèle, vous DEVEZ aussi augmenter votre sensibilisation. La tâche vous semble complexe ? C'est précisément l'une des priorités de Sirris et d'Agoria. Découvrez nos courts webinaires gratuits sur la confiance et la résilience (qui seront bientôt annoncés dans notre agenda) ou nos masterclasses pragmatiques, étape par étape, pour les concepteurs et les externalisateurs de services numériques. Nous nous engageons à vous fournir la meilleure formation possible!

Vous êtes un fournisseur de technologies numériques?

En 2021, les clients posent des questions sur la cybersécurité ; ils vous en poseront toujours plus! Nous avons pu vérifier qu'en travaillant avec des fournisseurs de technologie numérique, quelle que soit la technologie qu'ils fournissent, la majorité des entreprises reçoivent les questions suivantes de la part de leurs clients :

- Êtes-vous assez sûrs?
- Comment puis-je vous confier mes données en toute confiance?
- Quelles normes appliquez-vous?
- Avez-vous réalisé des tests de pénétration?
- Quel est votre niveau de sécurité?

L'aptitude à répondre à ces questions du client est souvent vitale pour mener des affaires. La confiance devient donc une priorité dans la continuité des activités des fournisseurs de services numériques. Comment faire? Pour les services numériques, il y a une excellente nouvelle : il existe en effet une solution très claire, à savoir devenir AppSec. Ceci signifie tout simplement appliquer les principes de la conception sécurisée dès le départ. Les principes sous-jacents sont connus sous le nom de « norme [ASVS](#) » (Application Security Verification Standard, norme de vérification de la sécurité des applications). À partir de cette norme, vous pouvez élaborer votre service en suivant les concepts DevSecOps. Vous trouverez plus d'informations à ce sujet ici. Vous pouvez également participer à notre masterclass sur la cybersécurité pour les concepteurs de services numériques.

Accroître la sensibilisation à la sécurité

Malheureusement, les interactions avec des tiers soulèvent souvent des questions relatives au facteur humain et à la confiance. Pour répondre à de telles questions ou les poser, vous devez posséder des connaissances en matière de sécurité. La matière peut sembler complexe ou effrayante, mais en pratique, il s'agit du moyen le plus économique et le plus rapide d'améliorer la sécurité. Il est moins coûteux et plus efficace de sensibiliser que d'acheter des outils et des solutions complexes (qui exigent à leur tour de nouvelles formations). La meilleure façon d'investir dans la cybersécurité consiste à investir dans une formation régulière ! Comment y parvenir de la

façon la plus judicieuse ? Sirris et Agoria proposent un éventail d'options:

- Webinaires gratuits sur la confiance et la résilience (bientôt dans notre agenda)
- Masterclasses avec une approche pratique, des conseils et un encadrement progressif:

]]>

Auteurs



Tatiana Galibus