Les RDV Experts

RISQUES CYBER - RGPD | DORA | NIS2

Le prestataire IT : maillon faible du risque cyber !

Dans le domaine de l'IT, les entreprises comme les établissements publics sont astreints à de nombreuses obligations. Mais il en est une qui est le plus souvent sous-estimée, voire ignorée : celle du recours à des prestataires tiers, les risques engendrés et les obligations que cela implique.

Il est rare, pour ne pas dire inexistant, pour un établissement quel qu'il soit de ne pas recourir aux services d'un ou plusieurs prestataires tiers, même dans les secteurs les plus sensibles. Les petites et moyennes entreprises font souvent appel aux services de MSP ou à des éditeurs de solutions logicielles en SaaS. Les ETI ou grandes entreprises, pour leur part, ont des kyrielles de contrats avec autant de prestataires.

Or, on assiste depuis quelques années au développement des cyberattaques de ces tiers pour atteindre le client final. C'est pour cela que l'Europe fixe un cadre juridique destiné à réguler les relations entre les entreprises et leurs prestataires.

Renforcement des exigences légales

Les premières exigences ont été fixées en 2016 par le RGPD pour les prestataires qualifiés de sous-traitants au sens du Règlement. Mais le législateur constate que huit ans plus tard, les entreprises n'ont pas compris ses attentes et que les mesures sont de la poudre aux yeux. Il vient, pour chacun des textes massues que sont DORA et NIS2, renforcer sa vision de la maturité cybersécurité et oblige un suivi en profondeur de la cybersécurité des prestataires tiers, tant au niveau gouvernance, juridique que technique.

Les entités essentielles et importantes doivent donc prendre toutes les mesures techniques, opérationnelles et organisationnelles appropriées et proportionnées pour gérer les risques qui menacent la sécurité de leurs réseaux et de leurs systèmes d'information.

Il s'agit là, comme le dit la directive elle-même, d'une approche « tous risques » qui porte notamment sur « la sécurité de la chaîne d'approvisionnement, y compris les aspects liés à la sécurité concernant les relations entre chaque entité et ses fournisseurs ou prestataires de services directs ».

Enfin, le Règlement DORA, qui sera applicable à compter du 17 janvier 2025, comporte un chapitre complet (Chapitre V) consacré exclusivement à la « Gestion des risques liés aux prestataires tiers de services TIC ».

Même s'il ne s'applique qu'aux acteurs du monde bancaire, financier et assurance, le Règlement DORA constituera à n'en pas douter un référentiel de bonnes pratiques pour tous les autres acteurs publics ou privés. Ce référentiel est également composé d'autres documents qui, sans être exclusivement juridiques, impactent la relation client/prestataire. Il en est ainsi des normes comme la suite 27000 ou des recommandations de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) ou de l'ENISA (Agence européenne de cybersécurité).

Votre cybersécurité repose sur vos sous-traitants : êtes-vous prêts ?

Pour explorer le sujet plus en détail et répondre à toutes les questions que vous vous (ou devriez) vous poser :

- A quels textes suis-je soumis ?
- Quel est le niveau de maturité attendu ?
- Quelles sont les sanctions encourues ?
- Quel référentiel appliquer ?
- Comment vérifier la conformité de mes prestataire IT ?
- Quelles sont les clauses contractuelles imposées ou impactées ?
- Quelles sont mes obligations en termes d'audit et leurs conséquences ?

Nous vous donnons rendez-vous le 19 mars à 10h pour un webinar inédit, animé par nos experts !

👉 **https://webikeo.fr/webinar/cybersecurite-impact-des-nouvelles-regles-europeennes-sur-vos-relations-avec-vos-prestataires-it**

Eric Barbry
Avocat Associé spécialisé IP/ IT
ebarbry@racine.eu

Marc-Antoine Ledieu
Avocat à la Cour et RSSI legal
marc-antoine@ledieu-avocats.fr

Jean-Philippe Gaulier
CEO de Cyberzen
jpg@cyberzen.com