wallix

02

Secteur bancaire : comment mieux maîtriser ses dépendances technologiques ?

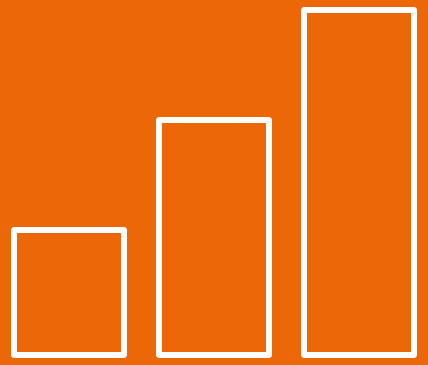


wallix

Les dépendances technologiques constituent un risque à la fois technique et stratégique pour le secteur bancaire.

De plus en plus des activités critiques sont externalisées : hébergement cloud, logiciels de cœur bancaire, traitement des paiements, cybersécurité, données de marché. Dans ce contexte, chaque fournisseur peut devenir un point de défaillance potentiel en cas de panne, de faillite ou de cyberattaque.

Ces dépendances technologiques deviennent encore plus sensibles dans le contexte géopolitique actuel. Beaucoup de fournisseurs étrangers sont soumis à des lois extraterritoriales et peuvent servir de leviers pour mettre la pression sur des acteurs nationaux ou industriels en cas de tension.



Toutefois, les dépendances technologiques ne sont pas une fatalité.

En suivant quelques démarches, les établissements bancaires peuvent apprendre à les maîtriser afin de gagner en souveraineté.

L'essentiel :

1

Cartographier ses dépendances (fournisseurs, technologies, données, compétences) et les relier aux fonctions critiques pour hiérarchiser les risques.

2

Diversifier de façon proportionnée : chercher des alternatives là où la criticité le justifie, et intégrer la souveraineté comme critère d'achat dès le départ.

3

Anticiper la sortie, comme l'exige DORA : scénarios, solution de remplacement, plan de migration, clauses contractuelles adaptées, et surtout des tests réguliers.

Première étape : Comment cartographier ses dépendances ?

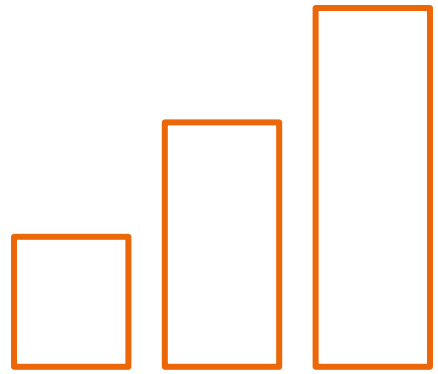
Pour gagner en souveraineté, il est important de bien connaître ses dépendances.

La première chose à faire est donc de les cartographier pour être en mesure de les identifier.

Cet inventaire doit couvrir plusieurs niveaux : les fournisseurs (hébergeurs, éditeurs, infogérants…), les technologies (services propriétaires, formats de données, API spécifique à un fournisseur…), les données (où sont-elles stockées ? Quelle juridiction ? Qui peut y accéder ?) et les compétences (quels savoir-faire sont détenus en interne ? Lesquels sont apportés par un prestataire ?).

wallix

Chacune des dépendances doit être reliée aux fonctions critiques ou importantes de l'établissement bancaire, afin de hiérarchiser les risques.



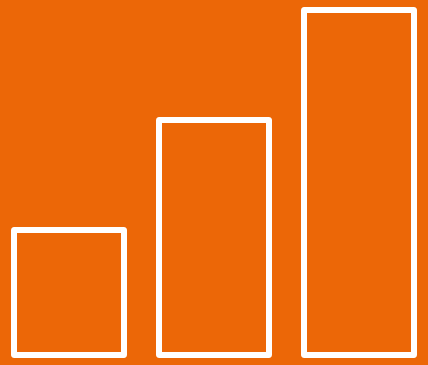
Quel serait l'impact d'une interruption ? Combien de temps faudrait-il pour la remplacer ? Existe-t-il une alternative réelle ? Le but de cette opération de cartographie est d'être capable d'apporter une réponse à ces questions.

Deuxième étape : diversifier les infrastructures et trouver des alternatives

La cartographie ainsi réalisée devient une base pour la seconde étape : diversifier les infrastructures et choisir des solutions qui réduisent la dépendance.

Le but de cette étape est de trouver des alternatives, européennes ou autres, afin de ne pas subir une interruption totale de l'activité en cas de tensions géopolitiques ou de sanctions liées à une juridiction extraterritoriale.

Pour réaliser cette étape, il est important de tenir compte du coût de cette diversification (complexité, compétence, exploitation), qui doit rester proportionné à la criticité des systèmes concernés.



Par exemple, pour un logiciel n'utilisant pas de données sensibles pour l'institution bancaire et ses clients, ce n'est pas forcément très grave de conserver un service en provenance d'un acteur soumis à une loi extraterritoriale.

Il ne s'agit donc pas de tout remplacer, mais bien de faire des choix stratégiques. Le critère de souveraineté doit être intégré dans les achats, au même titre que le prix, la performance et la sécurité, et non ajouté après coup.

Troisième étape : anticiper la sortie de la dépendance

Le règlement européen DORA exige des stratégies de sortie documentés pour tous les services relatifs aux technologies de l'information et de la communication soutenant des fonctions critiques ou importantes.

Concrètement, une stratégie de sortie crédible comporte : des scénarios précis (défaillance du fournisseur, dégradation du service, changement de juridiction, hausse de prix, sanction), une solution de remplacement identifiée (qu'il s'agisse d'un autre fournisseur ou d'un retour en interne), un plan de migration réaliste (avec des délais et des ressources) et la capacité à récupérer ses données dans un format exploitable.

wallix

Pour établir cela, le contrat est un levier clé négligé par beaucoup d'organisations, parce qu'il peut contenir des clauses de réversibilité, une assistance à la sortie, une durée de préavis, un format de restitution des données et des droits d'audit.

Enfin, il est primordial de tester la stratégie de sortie, même partiellement : si elle n'est jamais éprouvée, elle reste théorique et peut représenter quelques surprises le jour où on en a vraiment besoin.

wallix

En souveraineté, il n'y a pas de modèle unique.

Les établissements bancaires doivent donc faire les choix qui leurs sont adaptés, afin que la sécurité et le contrôle des dépendances ne deviennent pas une contrainte.

Chacun doit bâtir sa souveraineté à la mesure de ses activités et de ses enjeux.