KPMG

TIME TO ADAPT

COVID-19

La technologie, essentielle à votre continuité d'activité

Faire face efficacement

Contexte

L'épidémie de Covid-19 et la mise en place du confinement en France et dans d'autres pays a fortement impacté la vie des organisations:

- Un nombre important d'employés sont en télétravail
- Les consommateurs ne peuvent se déplacer que pour acheter des produits de 1ère nécessité.

Ces évolutions génèrent des **impacts et changements majeurs sur les infrastructures, outils et procédures** des organisations. Les accès au SI des organisations en télétravail se font désormais à l'aide de postes nomades connectés via Internet et les consommateurs ont **recours plus massivement aux services e-commerce.**

La bascule en télétravail ayant été réalisée parfois en urgence, il ne peut-être exclu que ces déploiements aient été **accompagnés d'une diminution du niveau de sécurité** des systèmes d'information. En outre, on note une **recrudescence des cyber attaques** (ransomware, phishing, DDoS) ces dernières semaines, certaines tirant parti de la vulnérabilité des personnes et des organisations.

Aussi, **la capacité à gérer cette situation sur le long terme soulève des interrogations** : casse ou panne des équipements nomades des employés, indisponibilité des collaborateurs IT clés, problèmes de performance, capacité des fournisseurs à délivrer les services attendus.

Enjeux pour assurer votre résilience

Dans cette situation exceptionnelle, les actions à entreprendre pour continuer les activités en mode télétravail et/ou e-commerce dépendent du degré de maturité et de préparation de chaque organisation.

1. Pour les organisations n'ayant pas initié ou finalisé la mise en place des moyens de télétravail et de e-commerce

- L'enjeu est de définir et déployer les moyens les plus adaptés pour permettre aux employés confinés de travailler et aux clients d'acheter les produits et de consommer les services.
- Ce déploiement doit être réalisé dans des conditions qui n'abaissent pas la sécurité de l'infrastructure et du SI et qui garantissent un niveau de performance acceptable.

2. Pour les organisations ayant mené des actions en urgence afin de déployer ces moyens

- L'enjeu est de sécuriser et de renforcer les infrastructures qui peuvent présenter des faiblesses de sécurité et de robustesse du fait des conditions des déploiements.

3. Pour les organisations qui avaient déjà des moyens et dispositifs de télétravail et e-commerce

- L'enjeu est de maintenir et d'optimiser les moyens en place, tout en faisant face à la recrudescence des cyber attaques, aux pics de charge dus à l'augmentation du nombre de personnes confinées et à l'attrition des matériels des télétravailleurs.

Des approches spécifiques à vos enjeux

Les équipes pluridisciplinaires de KPMG vous accompagnent avec des approches adaptées à votre contexte.

DEFINIR ET DEPLOYER LES MOYENS DE TELETRAVAIL ET DE E-COMMERCE 1

- **Identifier les applications, infrastructures et personnels clés** , et mettre en place des moyens de travail à distance (postes nomades et VPN, ou bureau virtuel)
- Identifier et déployer **des solutions de communication** et de collaboration en mode cloud
- Remplacer l'accueil physique des clients par une mise en relation numérique (**centre d'appel virtualisé, email, réseau sociaux, messagerie instantanée**).
- Permettre l**e paiement et la vente** en ligne, en adaptant les processus existant ou en mettant en œuvre une solution digitale
- Réaliser une rapide analyse de risque pour sécuriser le déploiement (**Security by design**).

SECURISER LES DISPOSITIFS DEPLOYES EN URGENCE 2

- Tracer **les dérogations et les entorses** à la politique de sécurité du SI (ouverture de flux, attribution de droits d'accès exceptionnels) dans une optique de maitrise des risques
- Pour les systèmes déployés ou modifiés en urgence (VPN, mail, cloud, vidéoconférence, partage de fichier, sites de vente en ligne) :
  - ✓ **Sécuriser** (authentification multi-facteurs, durcissement des configurations, etc.) et **tester** leur sécurité via notamment des tests d'intrusion
  - ✓ Analyser la **capacité** (matériel, licences) de tenue et de monté en charge des infrastructures IT
  - ✓ Assurer des **sauvegardes hors** ligne des systèmes critiques déployés ou modifiés en urgence
- **Sensibiliser** les utilisateurs aux nouvelles menaces liées au contexte actuel
- Dans le cas de BYOD, assister les utilisateurs dans la **sécurisation de leurs équipements personnels (MDM)**

ASSURER LA RESILIENCE DU DISPOSITIF DANS LA DUREE 3

- Identifier et anticiper **les facteurs de risques** pouvant impacter la continuité d'activité (cyber attaques, défaillance des systèmes IT clés, absence de personnel clé)
- Etudier les éventuels besoins **d'augmentation ou de réattribution des capacités** de l'infrastructure (système, réseau et fournisseurs), ainsi que les solutions alternatives (scaling cloud, répartition des charges horaires de connexion)
- **Assister les utilisateurs** (adaptation du support utilisateur, remplacement des matériels en panne et mise à disposition de bureaux virtuels)
- Adapter **les moyens de supervision** au nouvel environnement et modifier et renforcer les contrôles de sécurité (test d'intrusion), notamment sur les systèmes exposés sur Internet
- Surveiller l'éventuelle utilisation abusive du **shadow IT** par des utilisateurs

Nos atouts

Une capacité prouvée à construire des équipes pluridisciplinaires : technologiques (cloud), transformation, gestion de projet, conduite du changement, Cyber et Privacy, risques et spécialistes métiers, pour répondre aux demandes complexes de nos clients

Une capacité à dialoguer avec tous les niveaux d'interlocuteurs dans les organisations, de la Direction générale aux métiers et à la DSI.

Contacts

Laurent GOBBI
Associé Risk Consulting
Tél. : +33 6 14 58 91 00
Email : lgobbi@kpmg.fr

Vincent MARET
Associé Cyber Sécurité
Tél. : +33 6 17 12 22 13
Email : vmaret@kpmg.fr

Sébastien ROPARTZ
Associé Technology Transformation
Tél. : +33 6 60 10 02 58
Email : sropartz@kpmg.fr