KPMG

TIME TO ADAPT

COVID-19

Cybersécurité : protéger l'entreprise pendant et après la crise

Faire face efficacement

Les mesures de confinement et de distanciation physique décidées pour maitriser la pandémie Covid-19 ont montré la grande **importance des technologies numériques** (télétravail, e-Commerce, télémédecine, paiement sans contact, etc.) pour permettre une **poursuite de l'activité des entreprises**, même en mode dégradé.

Les entreprises sont aujourd'hui plus que jamais dépendantes des infrastructures numériques, et ce alors qu'on assiste à une **recrudescence des cyber attaques**.

Dans un contexte **de grande incertitude** quant au développement de la crise sanitaire, cette évolution vers le numérique des modes de travail et de consommation **est amené à perdurer**.

En sortie de crise, les entreprises auront à faire face à une **dette de sécurité et de conformité**, due aux impacts de la crise : changements urgents réalisés sur l'infrastructure, dérogations et entorses à la politique de sécurité, relâchement des contrôles.

En outre, la crise économique à venir engendrera dans un certain nombre d'entreprises une **pression importante sur les budgets** cyber.

Enfin, des facteurs multiples entraineront une **accélération et une systématisation des projets de transformation numérique** dans les entreprises : adaptation aux attentes des clients et des employés, renforcement de la résilience des processus, réduction des coûts, changement de business modèle.

Les enjeux de la cybersécurité et de la cyber résilience

Dans cette situation de crise, le défi principal pour les directions cybersécurité est d'assurer une protection optimale de l'entreprise contre les cyber menaces et les défaillances mettant en danger la continuité de ses activités, et ce dans des conditions très évolutives :

Résilience

Très court terme

L'enjeu est de protéger l'entreprise et les utilisateurs contre les cyber attaquants tirant parti du contexte de la crise (*phishing, ransomware*, etc.).

L'organisation et les dispositifs de continuité et de gestion de crise doivent notamment être adaptés afin d'assurer la continuité des activités si une nouvelle crise devait survenir.

Recovery

Court terme

L'enjeu est de s'assurer que le retour à des modalités de travail habituelles (présentiel, connexion au réseau local d'entreprise) se fait dans des conditions de cybersécurité acceptables et que les entorses aux règles de sécurité sont remédiées.

Il est également important de s'assurer que la fonction cybersécurité retrouve des capacités opérationnelles suffisantes et adaptées au contexte d'incertitude, notamment en tirant partie des leçons des mois passés.

New Realities

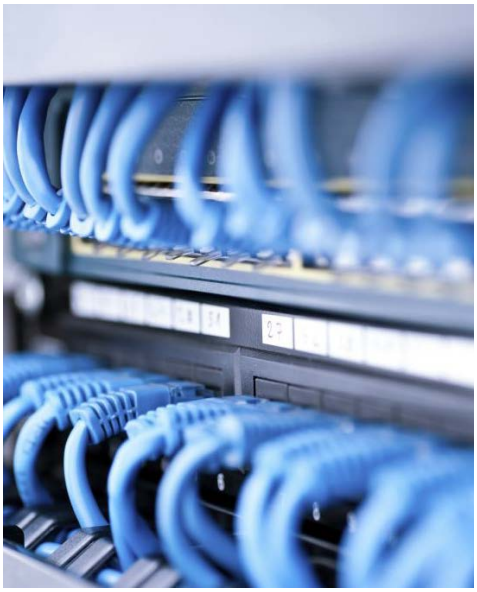
Moyen / Long terme

L'enjeu est d'adapter la *roadmap* et *l'operating model* de la cybersécurité afin de répondre pleinement aux besoins des métiers et attentes des clients (notamment dans les projets de transformation numérique) et de prendre en compte les impacts économiques sur les moyens alloués à la cybersécurité.

De nouvelles priorités pour les équipes cybersécurité

1. Maintenir l'activité durant la crise en gérant les risques

S'assurer de la résilience et de la sécurité des infrastructures et des applications critiques accessibles sur Internet (VPN, serveurs mail, visioconférence, partages de fichiers, outils de sécurité, applications métiers...)



Evaluer 1

les capacités de montée et de tenue en charge (matériel, licences) de l'infrastructure. Si besoin, augmenter ou réattribuer les capacités, étudier des solutions alternatives (avec changement de fournisseurs si nécessaire) et renégocier les contrats auprès des fournisseurs et prestataires

Tester 2

le niveau de sécurité des environnements accessibles depuis Internet (tests d'intrusion, scans de vulnérabilité, revues de configuration, revues d'architecture, etc.)

Renforcer 3

la sécurité des environnements nouvellement ouverts sur Internet (authentification forte, contrôle d'accès, surveillance, etc.)

Adapter 4

au contexte de crise (travail à distance, effectifs réduits) les procédures opérationnelles de gestion et de supervision de la cybersécurité (correctifs, sauvegardes, anti-virus, surveillance)

Tracer 5

les dérogations et les entorses à la politique de sécurité du SI, dans une optique de maîtrise des risques et de maintien de la conformité

Surveiller 6

la surface d'exposition de l'entreprise sur Internet, notamment les infrastructures déployées en urgence (cloud et Shadow IT)

De nouvelles priorités pour les équipes cybersécurité

Gérer les nouveaux risques et éviter les sur-incidents

1 Réévaluer

les risques IT et cyber au regard de la crise Covid-19 (cyber attaques, défaillance de systèmes IT clés absence de personnel clé)

2 Analyser

les capacités de réponse à de nouvelles crises : sauvegardes et restaurations, disponibilité des personnes et des outils, adéquation des procédures, SLA des fournisseurs

3 Mettre à jour

les plans de continuité informatique et métier, en vérifiant notamment la capacité de déploiement à distance

Sensibiliser et aider les collaborateurs

1 Sensibiliser

les collaborateurs aux risques et bonnes pratiques liés au contexte de crise (fiches de bonnes pratiques, e-learning, campagne de phishing)

2 Aider

les collaborateurs à sécuriser leurs pratiques dans un contexte de télétravail, avec dans certains cas, l'utilisation de matériels et de services non professionnels

KPMG

2. Assurer la sortie de crise et rétablir un dispositif de cybersécurité adapté

Préparer et piloter le retour à l'état nominal du système d'information et de la posture cybersécurité

1 Evaluer

l'étendue de la dette de cybersécurité / privacy qui s'est constituée durant la crise sanitaire

2 Réaliser

un « health check » cybersécurité des systèmes, dans un contexte de reprise d'activité nominale (stations et smartphones des collaborateurs, applications métier, infrastructures externes, outils de sécurité)

3 Analyser

et scanner tous les équipements avant de les rebrancher sur le réseau interne de l'entreprise

4 Relancer

les éventuels processus cyber interrompus temporairement (sauvegardes, correctifs, habilitations, etc.), en les adaptant à un contexte qui reste dégradé par rapport à la situation antérieure

5 Contrôler

les sauvegardes (notamment en faisant des tests de restauration)

6 Effectuer

une revue des fournisseurs IT et Cyber pour prendre en compte les incapacités et insuffisances

7 Rapatrier

les données stockées hors des systèmes de l'entreprise (ordinateurs personnels, stockage cloud, clés USB privées).

8 Chercher

des traces d'intrusion non détectées dans le SI (threat hunting)

La « dette » de cybersécurité Covid-19

- Dérogations et entorses à la politique de sécurité
- Mise en production d'applications sans analyses de risques ou tests de sécurité préalables
- Ouverture accélérée de flux sur les pare-feu
- Attribution de droits d'accès exceptionnels aux utilisateurs
- Acceptation de non-conformités aux réglementations
- Mises à jour ou correctifs non installés sur les serveurs et les postes de travail
- Stations de travail infectées durant le télétravail
- Audits de sécurité non réalisés
- Données de l'entreprise stockées sur des dispositifs personnels ou non sécurisés
- Utilisation de services shadow IT
- Installation de logiciels non professionnels
- Autorisation d'utiliser les ports USB sur les stations de travail
- Désactivation des solutions d'authentification forte
- Règles de pare-feu désactivées
- Services exposés sur Internet (RDP)

Tirer les leçons de la crise sanitaire

Analyser 1

les mois de crise Covid-19 passés et identifier les besoins métier, sécurité, conformité et privacy auxquels les modes de travail dégradés n'ont pas pu suffisamment répondre pendant la crise (travail à distance, solutions de communication et de collaboration, échanges dématérialisés avec les clients et les partenaires, paiements, ventes et facturations en ligne, accès aux applications métiers, etc.)

Adapter 2

l'organisation, les politiques, les procédures opérationnelles et les plans de continuité en tenant compte des expériences acquises pendant la crise (systèmes et personnes clés, continuité des équipes et des systèmes de cybersécurité, maintien d'un socle minimal de sécurité, gestion d'une sur-crise à distance)

Evaluer 3

les applications et solutions, notamment collaboratives, acquises et déployées en urgence, dans une optique de confirmation, de remplacement ou de sécurisation.

Initier le transformation de la fonction Cyber pour s'adapter au nouveau contexte

- Quick wins pour réduire et rationaliser les coûts cybersécurité
- Implication dans les premières initiatives métiers de digitalisation en sortie de crise
- Insertion dans les programmes de résilience d'entreprise

KPMG

3. S'adapter au monde post-crise et assurer l'alignement sur la stratégie de l'entreprise

Transformer la filière cybersécurité dans l'entreprise pour l'adapter aux nouvelles réalités

Revoir 1

la cartographie des risques cyber au regard du nouveau contexte, et identifier les zones de risques prioritaires

Réévaluer 2

le portefeuille de projets cyber, en termes d'apport à la maîtrise des risques et d'alignement à la nouvelle stratégie de l'entreprise,

Adapter 3

la posture cybersécurité au nouveau contexte, notamment en terme de roadpmap, de security operating model et de mesures de sécurité avec un objectif de rationalisation

Rationaliser 4

le catalogue des mesures techniques, procédurales et organisationnelles de sécurité, dans une optique d'efficacité et d'efficience

Automatiser 5

les activités de sécurité (gestion des vulnérabilités et correctifs, détection et traitement des attaques), en développant notamment des capacités d'IA.

Etudier 6

la possibilité d'externaliser les opérations de sécurité : cloud, managed services

Sélectionner 7

les CAPEX/OPEX cyber prioritaires dans un contexte de pression forte sur les coûts

Adapter 8

le reporting afin de démontrer l'efficacité des investissements cyber et l'alignement sur la stratégie de l'entreprise

Anticiper et accompagner les projets de transformation numérique de l'entreprise

Accompagner 1

proactivement l'entreprise dans les projets de transformation numérique lancés pour s'adapter aux nouvelles réalités, en se positionnant comme un « business enabler »

Intégrer 2

le "Security / Privacy by design" dans les projets de transformation numérique et les processus de développement, afin d'assurer une prise en compte des risques cyber dès l'initialisation des projets

Collaborer 3

avec les métiers pour développer des moyens permettant d'assurer un niveau de sécurité et une expérience utilisateur adaptés aux attentes des clients

Observer 4

les évolutions des attentes des consommateurs, des business models, des technologies, des risques et des réglementations, afin d'anticiper les impacts pour la cybersécurité

Accompagner les programmes de résilience de l'entreprise, face aux crises sanitaires ou autres

Intégrer 1

le domaine cybersécurité dans le programme de résilience opérationnelle de l'entreprise

Préparer 2

et simuler des crises cyber dans des contextes multi-crises

Evaluer 3

l'adéquation de la couverture de la cyber assurance

Renforcer 4

les contrôles sur les fournisseurs et sous-traitants : cybersécurité, résilience, capacité à délivrer

KPMG, un leader global en cybersécurité

KPMG, au côté des entreprises pour maitriser les risques cyber

- Une capacité prouvée à construire des équipes pluridisciplinaires (experts Cyber et Privacy, spécialistes métiers, technologies, risques, innovation, conduite du changement) pour répondre aux demandes complexes de nos clients
- Des prestations Cyber bénéficiant d'une expertise technique poussée, d'une connaissance approfondie des métiers, des risques et des contraintes réglementaires,
- Une capacité à dialoguer avec tous les niveaux d'interlocuteurs dans l'entreprise, de la Direction générale aux métiers, des fonctions de contrôle aux experts techniques
- Une capacité à mettre les risques cyber en perspective avec les métiers, l'organisation et la culture de nos clients, permettant aux parties prenantes de prendre des décisions
- Une garantie de confidentialité, une rigueur méthodologique et une qualité de reporting élevée et constante
- Une indépendance par rapport aux prestataires de service, fournisseurs de solution et aux intégrateurs

Une expertise technologique

- Des laboratoires de cybersécurité KPMG regroupant des expertises techniques de pointe et certifiées (PASSI, CHECK, CREST, SANS, OSCP, CISSP, ISO27001)
- Une expertise couvrant tous les types de SI : gestion, scientifiques et techniques, logistiques, IoT, industriels
- Un focus spécifique sur le conseil en innovation technologique et sur la gestion des risques dans les technologies émergentes (IA, RPA, blockchain...)

Un réseau international

- Une coopération poussée entre les plus de 3 200 experts Cyber et Privacy de KPMG dans le monde (groupes de travail, formations, thought leadersphip…)
- Une vision globale de l'état de l'art et des meilleurs pratiques en matière de gestion des risque cyber, nourrie par des interactions avec des centaines de clients dans le monde entier, et une capacité à construire des benchmarks
- Une capacité d'intervention internationale grâce à des équipes Cyber et Privacy présentes dans 50 pays et une gestion coordonnée des clients globaux

Contact

Vincent MARET
Associé, responsable cybersécurité et Privacy
Tel. : +33 6 17 12 22 13
Email : vmaret@kpmg.fr