TECHNOLOGIE
UN ATOUT INCONTOURNABLE POUR LA RÉSILIENCE ORGANISATIONNELLE

KAVISH DUSSOYE EXECUTIVE – TECHNOLOGY AND SERVICES, BIRGER.

LA CRISE SANITAIRE A CONFIRMÉ L'IMPORTANCE DE LA TECHNOLOGIE AU SEIN DES ENTREPRISES. LA RÉSILIENCE ORGANISATIONNELLE EST AINSI DEVENUE PRIMORDIALE POUR ASSURER LA CONTINUITÉ DES ACTIVITÉS DANS CETTE NOUVELLE RÉALITÉ. LA PRUDENCE ET LA SÉCURITÉ RESTENT CEPENDANT DE MISE.

L'IMPACT économique de la crise sanitaire est irréversible. La pandémie a eu un effet négatif à long terme sur les économies de par les mesures de restriction et le confinement imposés à une grande partie de la population mondiale, entraînant un arrêt économique brutal, avec une chute des activités productives. Cependant, les conséquences négatives ont été atténuées par l'adoption de la technologie. Pour faire face à ce contexte turbulent et incertain, les entreprises ont dû élaborer des stratégies de résilience pour devenir agiles face aux difficultés des opérations pour maintenir la continuité de leurs activités. Du jour au lendemain, les employés ont dû adopter le télétravail avec la mise en place des outils nécessaires en utilisant les technologies telles que le cloud, le VPN (réseau privé virtuel) et les plateformes de collaboration.

Toutefois, ces initiatives de travail à distance ont exposé les entreprises à de nouveaux défis sécuritaires car le mode d'opération a évolué de circuit fermé à un qui est plus ouvert. Cette approche de travail a augmenté la vulnérabilité de la surface d'attaque des entreprises face aux cyber-menaces. Cela dit, cette réalité préoccupante nécessite de prendre des mesures d'urgence et d'implémenter des technologies avancées pour protéger les surfaces d'attaques des entreprises. Pour cela, les entreprises doivent premièrement transférer leur première ligne de défense sur des passerelles de sécurité hors de leur périmètre de défense traditionnelle pour mieux se protéger. Néanmoins, elles doivent prendre en compte la protection de leurs infrastructures internes qui sont plus à risque. Il est donc aussi important de protéger cette seconde ligne de défense à l'aide de technologies appropriées telles que les antivirus ou les solutions EDR (Endpoint Detection and Response) ; des logiciels de chiffrement des données ; des pare-feux de nouvelle génération ; des solutions DLP (Data Loss Prevention) et des solutions pour la gestion des identités avec accès Zéro Tolérance (ou Zero Trust).

À la suite de nos enquêtes de cybersécurité, nous avons constaté que les cybercriminels utilisent les mêmes vecteurs d'attaques et s'adaptent à la nouvelle façon d'opérer des entreprises dans l'ère de la pandémie Covid-19. Les répondants de nos enquêtes nous ont d'ailleurs confirmé que le facteur humain est le maillon le plus faible. Le volume d'attaques généré submerge les équipes de sécurité des entreprises et leur manque de ressources appropriées (financières et humaines) est un défi important pour elles. Pour ces raisons, nous avons recommandé aux entreprises de sensibiliser leurs employés et de promouvoir l'utilisation de l'automatisation en s'appuyant sur l'intelligence artificielle pour traiter rapidement de grandes quantités d'informations afin de prendre des actions correctives appliquées automatiquement.

RÉSILIENCE ORGANISATIONNELLE

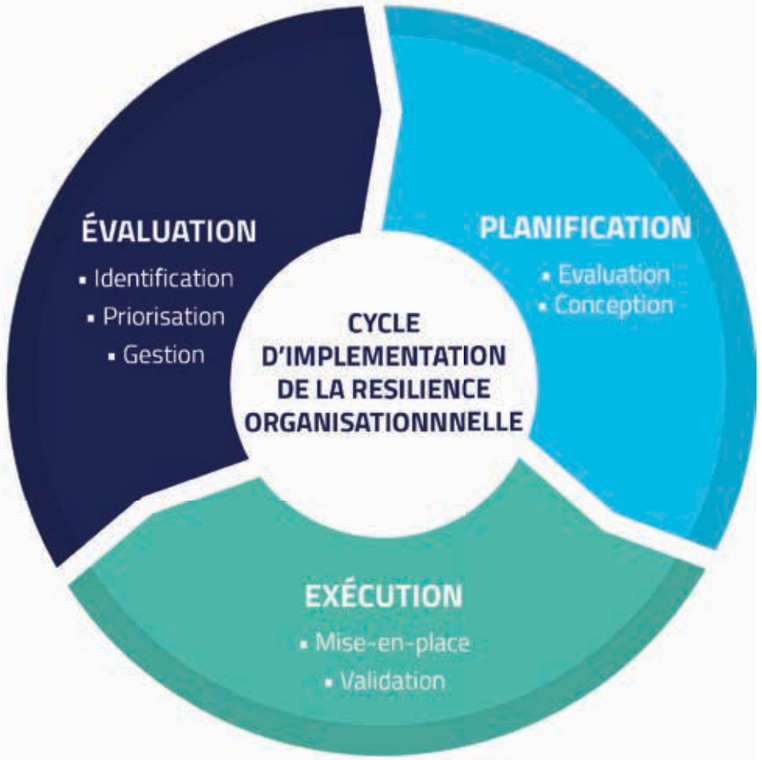
Cette crise sanitaire et économique perdurera, et leurs conséquences pour les entreprises seront importantes. Et comme mentionné plus haut, les risques de cyberattaques ont augmenté et il est envisageable que les cyberattaques pourraient être à l'origine d'une prochaine crise financière globale. Il est donc impératif que les entreprises de tous secteurs prennent conscience de l'importance de la résilience organisationnelle et de son cycle d'implémentation pour assurer leur croissance. Pour s'adapter et survivre dans cette nouvelle réalité, il est primordial d'inculquer une philosophie de la résilience à tous les collaborateurs de l'entreprise. Automatiser la continuité des activités en s'appuyant sur les technologies robustes, protégeant les données et délocalisant géographiquement les opérations pour pérenniser les entreprises sur le moyen et long termes.

Les données sont une ressource indispensable pour les entreprises, et il est donc impératif de considérer leur sauvegarde utilisant une approche 3-2-1 (trois copies de données, deux types de stockage différents et une copie hors site). La réplication hors site en temps réel des données assurera la reprise des activités rapidement en cas d'incident disruptif. Un Plan de Continuité d'Activité (PCA) contribuera à soutenir cette stratégie et l'ensemble des dispositions définies en cas d'incident par l'entreprise garantira la continuité de ses activités.

Par ailleurs, gérer et assurer la coordination des procédures associées des parties prenantes demeurent aussi une tâche très complexe. Il faut alors s'appuyer sur une technologie robuste et implémenter les outils nécessaires qui accompagneront l'entreprise dans la mise en place de son PCA ; tout en analysant les risques en amont, tester le PCA et le mettre à jour. Il existe aujourd'hui des outils de PCA qui permettent d'orchestrer le basculement des systèmes vers les sites de replis automatiquement tout en établissant la collaboration des équipes. Une fois en place, l'équipe de crise pourra entreprendre ses tâches prédéfinies pour qu'elles prennent les actions prioritaires tout en assurant le suivi des opérations jusqu'à la reprise des activités de l'entreprise.

Pour rappel, la semaine dernière a été dédiée à la Sensibilisation à la Continuité d'Activité dans le monde. Nos recommandations ont été de sensibiliser régulièrement nos collaborateurs à travers des formations continues. Nous les avons initiés à investir dans des technologies adaptées pour assurer la Résilience Organisationnelle et solliciter les Sociétés de Services Spécialisées pour pallier le manque de compétences et les restrictions budgétaires.

Au final, on peut dire que bien plus que la dernière solution à la mode, le digital est un changement d'approche qui concerne tant les outils de travail que la stratégie qu'ils permettent de concrétiser. C'est une réflexion qui doit se faire sur les objectifs stratégiques, soutenue par un plan de croissance élaboré ainsi qu'un plan de continuité d'activité dynamique. À juste titre, les solutionschoisiesseront adaptées, et pourront accompagner la modernisation de l'entreprise en toute fluidité.



«LES CYBERATTAQUES POURRAIENT ÊTRE À L'ORIGINE D'UNE PROCHAINE CRISE FINANCIÈRE GLOBALE»