

## Gérer une dynamique de Résilience globale

### Comment protéger efficacement mon système d'information ?

Pour répondre correctement à cette question, la première étape consiste toujours, pour nous chez eBRC, à en poser quelques autres :

- Quel est l'objectif réel : protéger une infrastructure informatique... ou plutôt protéger les activités que cette infrastructure supporte ?
- Par rapport à ces activités, comment se présente le paysage des risques auxquels il faut faire face ?
- Pour ces divers risques, quels sont les impacts en cas de problème réel ?
- Par rapport à ces enjeux, quels sont les budgets qui peuvent être consacrés à la protection ?
- Par rapport à ces budgets, quelles protections mettre en œuvre pragmatiquement pour assurer le juste arbitrage coûts/bénéfices ?

Notre approche holistique tient compte de l'impact de la sécurité et de la conformité à travers toute les couches de l'organisation d'une entreprise : ses réseaux et son infrastructure informatique, ses applications et informations, la conformité et la gouvernance. La technologie est importante, mais il faut tenir compte des personnes, des processus et de la réglementation afin d'élaborer une Politique globale de sécurité

### Avant de penser à son infrastructure IT et à la sécurité qui l'entoure quelle est la vision globale que doit avoir une entreprise, quels sont les préalables à ne surtout pas manquer pour protéger au mieux justement cette infrastructure ?

La vision globale de la sécurité opérationnelle prend sa source dans la politique d'ensemble de l'Entreprise : elle constitue un chapitre important de la charte de « Corporate Gouvernance », parce qu'elle y formalise les engagements pris par l'Entreprise pour garantir effectivement à ses clients les niveaux de service qu'elle leur annonce.

Sur cette base, on peut alors conduire des analyses d'impact, qui vont détailler progressivement les risques et les conséquences d'un incident se produisant dans la chaîne IT, et ce en relation directe avec les ambitions de la « Corporate Gouvernance ». Si votre métier est le transport des diamants bruts (une activité encore souvent réalisée au moyen d'un billet d'avion et d'un Attaché-Case ordinaire!), votre dépendance vis-à-vis de l'IT est nulle, comparée de celle de l'aéroport dont la logistique des bagages repose entièrement sur l'informatique... ce quelle que soit par ailleurs la valeur respective des contenus, bien entendu. Chaque « Métier » présente ainsi ses propres profils de risque ; les connaître permet d'aller droit à l'essentiel.

Après avoir trié les résultats des analyses d'impact par ordre d'importance et avoir défini les budgets disponibles, les départements concernés sont amenés à contribuer à la définition de Plans de Résilience pragmatiques et vérifiables. Ces plans doivent être alignés entre eux et consolidés en un tout cohérent. Ils débordent aussi de plus en plus largement du cadre de l'IT au sens des TIC. Les facteurs humains sont fondamentaux dans un plan de résilience : rien ne sert d'avoir des équipements de secours bien abrités dans un bunker si les seuls informaticiens capables de les mettre en services sont bloqués dans les bouchons consécutifs à la panne électrique générale !

Enfin, avant même de passer au déploiement du Plan, il est extrêmement important, pour la notion même de Résilience, de

considérer l'ensemble de cette démarche sous un angle dynamique. Non seulement les conditions extérieures changent, ainsi d'ailleurs que le métier lui-même, ce qui impose de refaire régulièrement le point et de corriger le cap. Mais surtout, la dynamique doit être inscrite dans les Plans, sous forme de critères d'avancement des déploiements, d'évaluation des tests, et d'indicateurs continus du niveau de contrôle des risques. On le voit, ceci revient somme toute à considérer la Résilience comme un processus de production comme un autre.

**Vous aidez donc les entreprises à identifier leurs risques business et l'impact de chaque risque... De quelle manière eBRC intervient-il lorsque l'on rentre plus dans les détails de l'IT proprement dite ?**

Sous l'éclairage du point de vue global, les divers Plans de Résilience vont faire apparaître des besoins spécifiques, plus directement liés au traitement de l'information, en effet. Ici, eBRC propose un ensemble de « produits » dans lesquels nos clients peuvent puiser pour réaliser ou compléter leurs Plans de Résilience.

Notre vocation consiste avant tout, à ce niveau de mise en œuvre, à proposer des « produits de services » qui peuvent réellement profiter des effets de levier en mutualisation et en industrialisation parce qu'ils supposent des investissements lourds en équipements, en outils et en compétences. Quelques exemples évidents :

- Centres de traitement hautement résilients (puissance électrique, refroidissement de niveau Tiers 4) accessibles de la demi-baie ...à plusieurs centaines de mètres carrés ;
- Positions de travaux riches, avec service de mise en œuvre accélérée entièrement sur mesures (postes de travail, basculement voix et data...)
- En partenariat avec le Groupe EPT, des liens redondants au niveau Térabit avec les principales capitales européennes ;
- Plateforme de Monitoring continu de processus complexes, avec notification d'alertes automatique
- Co-gestion de plateforme applicative
- Expertise en déploiement de Salles Informatiques complexes ;
- Expertise en gestion de Tests de Plans de secours ;
- Hébergement de données critiques ;
- Mise à disposition d'équipements de secours, ou de Centre de Crise...

**Vous serez d'accord que pour mieux sécuriser son infrastructure IT il faut pouvoir la contrôler en permanence, comment cela peut il se faire efficacement si une partie ou la totalité de celle-ci n'est pas sur place ?**

Nous avons mentionné ci-dessus un « produit » particulier dans notre portefeuille : notre Plateforme de Monitoring continu de processus complexes, avec notification d'alertes automatique. Cette Plateforme, déployée sur un modèle classique 3 tiers sur base d'agents de collecte sécurisés, est entièrement flexible (elle n'est pas limitée à la surveillance de composants informatiques, d'ailleurs) et a été conçue dès le départ pour assurer la surveillance de sites distants.

C'est exactement ce que nous avons fait lorsqu'eBRC a assuré le monitoring constant des infrastructures IT mises à la disposition des instances gouvernementales lors des 6 mois de la Présidence.lu. Dans ce cas, un partie des infrastructures étaient même mobiles, démontées le soir dans un château pour être remontées le lendemain dans une abbaye ! Pas une seule attaque n'a pu mettre cette plateforme multi-sites en péril !

Pour nous, d'ailleurs, un Client hébergé chez eBRC n'est en rien différent d'un Client distant : l'infrastructure de connexion sécurisée est identique, la seule différence étant... le coût de la ligne externe, dans le second cas. Et dans les deux cas, nous

voulons donner au Client une visibilité aussi large que possible sur la santé de sa plateforme. Nous déployons donc systématiquement un Cockpit qui intègre l'ensemble des informations de manière structurée, avec un espace de collaboration virtuel, cockpit auquel le Client a un accès sécurisé par Token. Il reste ainsi très proche de ses équipements, dans tous les cas.

Tous les spécialistes s'accordent à dire qu'il n'est plus possible de suivre en détail le flux croissant d'évènements constatés sur les plateformes modernes : trop d'évènements, trop de formats différents, vulnérabilités en mutation permanente, écart grandissant entre les aspects techniques et les besoins fonctionnels des métiers, etc. Certes, des outils existent, mais leur coût d'acquisition et de maintenance est important, et ils exigent de sérieux efforts de configuration, d'évolution et d'expertise.

A ces contraintes, eBRC répond par la mutualisation d'outils et d'expertises, offrant un service d'analyse, exactement comme le ferait un laboratoire d'analyses médicales. En entrée, les "échantillons" prélevés sur la plateforme du client, où qu'elle soit ; en retour des index lisibles, qui permettent un diagnostic précis et une thérapie efficace.

Que ce soit à distance ou dans nos murs, le grand avantage de notre service de Monitoring est que nos clients ne doivent plus maintenir en permanence l'intelligence de l'outil, chacun pour son compte. Laisse à lui-même, un outil de monitoring meurt en 6 mois ; sa gestion demande des ressources importantes et très spécifiques, que peu de clients peuvent maintenir en continu. Chez eBRC, par contre, maintenir l'intelligence de notre plateforme fait partie intégrante de notre métier !

