

Une Présidence .eu orientée «continuité des services»

De janvier à fin juin 2005, eBRC a assuré l'audit et le monitoring permanent de la sécurité informatique du réseau de la Présidence luxembourgeoise du Conseil de l'Union européenne. Un contexte inédit, mais résolument orienté «continuité des services» pour le spécialiste de la résilience.

Plus de cinq cents réunions en six mois; certaines d'un jour, les plus longues s'étirant sur trois jours. A certains moments, jusqu'à sept sites étaient

opérationnels en même temps, à d'autres plusieurs installations ont été réalisées dans la même journée. Pour eBRC, qui a assuré les audits préventifs et le monitoring permanent de la sécurité de la plateforme du réseau de la Présidence luxembourgeoise du Conseil de l'Union européenne, le défi tenait assurément aux impératifs de mobilité et de délais imposés par le Gouvernement.

Sous la conduite de l'EPT, le projet informatique lié à la Présidence européenne a réuni de nombreux partenaires, chacun prenant en charge un segment bien défini de la solution. On l'imagine, un des points

névralgiques tenait assurément à la sécurité d'une plateforme complexe, servant des acteurs divers et exigeants, et de surcroît fort exposée: mission -à tout le moins critique- qui fut assurée par eBRC avec un souci constant de continuité et de qualité.

Aujourd'hui, près de trois mois après la fin de la Présidence, le bilan tient en trois mots: rien à signaler! De fait, pas le moindre incident significatif n'est venu perturber le bon déroulement des réunions. Tout a parfaitement bien fonctionné, en toute sécurité... Mais n'était-ce pas l'objectif recherché?

A travers ce projet, eBRC a pu mettre en œuvre deux services de résilience d'activité. A savoir le monitoring à distance, en continu, des périmètres de sécurité des sites d'échange de communication et les services d'audit préventif.

Pratiquement, le gros du travail a débuté trois mois avant la Présidence. A l'automne 2004 donc, eBRC a défini avec les différents partenaires un ensemble de règles de fonctionnement et de procédures à suivre. Globalement, la difficulté tenait moins aux technologies de communication mises en œuvre -notamment wireless et streaming- qu'aux conditions de travail. En effet, certains sites se prêtaient mal à une sécurisation, voire même au déploiement du câblage. On songe ici, par exemple, à l'épaisseur des murs du Château de Vianden. Ou, sur d'autres sites, à la nécessité de remplacer des fenêtres! D'autre part, le travail des délégations ministérielles imposait des contraintes particulières, dont celle, assez inédite, de ne pas... imposer trop de contraintes! Il a donc fallu être créatif pour fournir un espace de travail à la fois convivial, ouvert, efficace et sûr.

En même temps, eBRC a défini les conditions de réception des plateformes -avant mise en production (audit préventif). Au départ d'une «security policy» unanimement partagée, eBRC a profilé deux schémas d'investigation: White Box et Black Box. Le premier reposait sur la connaissance de l'environnement et

la possibilité d'accéder aux machines, alors que le second reposait sur des tests de pénétration de l'extérieur sans droits d'accès à l'environnement. Ces audits -menés avant et pendant la Présidence- ont permis aux partenaires en charge des déploiements d'apporter aussitôt les corrections nécessaires.

Tout aussi stratégique, la mission de monitoring en temps réel. Elle reposait sur la plateforme Remote Monitoring de eBRC, un outil entièrement développé au Luxembourg, les services étant assurés en fonction des horaires imposés par le Gouvernement. Ici encore, les partenaires étaient avertis des moindres anomalies et pouvaient réagir en temps réel. Le travail d'analyse, de corrélation des logs et des événements était permanent. Pour ce faire, eBRC s'est basé sur la plateforme MSS (Management Security Services) de collecte d'alerte Virtuoso-développé au Luxembourg-, l'objectif étant de remonter les informations pertinentes afin de réagir vite et, surtout, efficacement.

S'il fallait résumer par un mot les leçons de ce projet, c'est bien «réactivité». Rarement les différents partenaires ont dû travailler dans des conditions aussi strictes en termes de mobilité et d'urgence -chaque utilisateur final devant disposer, que le site soit fixe ou mobile, d'une configuration informatique, systèmes d'impression et de copie compris, comparable à celle d'un bureau, plus l'avantage de profiter d'une bande passante à tout le moins confortable. Un demi-millier de réunions en six mois c'est autant d'installations des équipements, de tests avant le démarrage des PC; c'est autant de procédures de suivi, d'audits et d'analyses. Bref, par-delà les procédures liées à la sécurité même du projet, il fallait tenir compte d'un énorme travail d'organisation et de logistique. Qui plus est, ce fut un projet inédit, à mener sur une période courte prédéterminée. Et pour lequel le droit à l'erreur avait été banni -avant même de commencer. Il en allait de l'image de marque du Luxembourg.



MSS by eBRC

Dans le cadre de sa mission en continuité des affaires, eBRC propose des services mutualisés d'assistance opérationnelle en sécurité. Ces services ont pour objectif de mettre à disposition des clients, à distance, les ressources (connaissances, savoir-faire et outils) et les processus industriels de gestion requis pour renforcer la sécurité opérationnelle des flux d'information.

Ces services se situent dans une perspective globale visant à maintenir les chaînes d'applications «métier» (systèmes, réseaux, applications) dans un état continu de disponibilité et de robustesse face aux risques de défaillances techniques ou de violations malveillantes.

Ces services MSS (Managed Security Services), qui tournent en continu 24 x 7 x 365, sont livrables à deux niveaux:

- Monitoring Only: analyse des événements générés par les flux surveillés et la plateforme informatique sous-jacente et notification des alarmes résultantes;
- Full Management: gestion complète des composants de sécurité, tant proactive que réactive, y compris leur monitoring.

Toutes les communications (remontées de log, actions...) sont sécurisées et authentifiées. Ces services sont entièrement et exclusivement élaborés, opérés et livrés à partir du territoire du Grand Duché de Luxembourg, l'atelier d'analyse, de corrélation et de notification étant sous le contrôle complet d'eBRC, pour assurer la meilleure adaptation aux besoins des clients.



© Tom Wagner/Agence 2005.lu