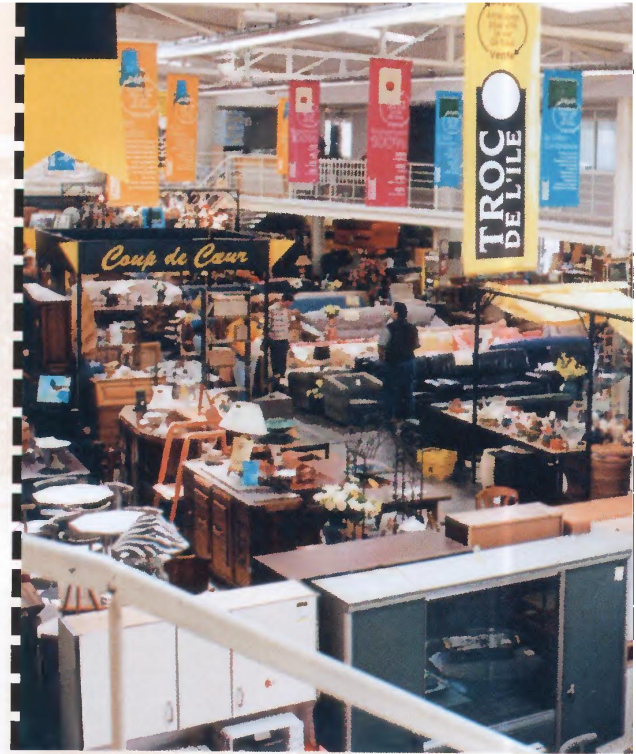


Rationalisation, homogénéisation puis consolidation des infrastructures ne se suffisent plus à elles-mêmes. Il faut ajouter une couche de supervision et de sécurité. Une approche qui passe aussi par l'infogérance.

# Sécurité et supervision deviennent impératives



**R**épondre au manque de flexibilité et d'adaptabilité, à la prolifération des serveurs et améliorer la qualité de service et la sécurité : toutes ces bonnes raisons ont incité les DSI à engager des actions pour faire évoluer leurs infrastructures, matérielles et réseaux. Le phénomène n'est pas nouveau et les DSI ont connu plusieurs vagues. Après une vague de rationalisation (réduire le nombre de machines), d'homogénéisation (standardiser les serveurs et les postes de travail), puis de consolidation/centralisation, les préoccupations liées à la sécurisation et à la supervision se renforcent. Le besoin de supervision est d'autant plus crucial que les parcs sont importants. Ainsi, l'ANPE, pour gérer ses 102 000 matériels répartis sur plus de mille sites, a décidé de rationaliser ses processus et a opté pour une solution (EasyVista de Staff&Line) destinée à inventorier automatiquement le parc et à modéliser (avec un moteur de *workflow full Web*) les procédures de validation. Les clients internes (directeurs d'agence, directeurs régionaux...) ont accès à un portail utilisateurs les autorisant à visualiser leur parc, gérer leurs commandes, inventorier leur région ou leur agence.

## Industrialiser les bonnes pratiques

L'autre aspect concerne la sécurité. Et sur ce terrain, l'enjeu est de disposer d'infrastructures à haute disponibilité. Cela conduit nombre d'entreprises à recourir à l'infogérance parce que le traitement en interne se révèle vite complexe. "Malgré le soin



**GILLES CAPELLA,**  
DIRECTEUR INFORMATIQUE  
DE TROC DE L'ÎLE :  
"Malgré le soin apporté à la sauvegarde des informations, un de nos magasins a perdu ses données comptables, impliquant un travail de ressaisie de près de deux mois. Il était donc nécessaire de recourir à un service de sauvegarde externalisé."

apporté à la sauvegarde des informations, un de nos magasins a perdu ses données comptables, impliquant un travail de ressaisie de près de soixante jours. Il était donc nécessaire de recourir à un service de sauvegarde externalisé plutôt que de traiter la question en interne", précise Gilles Capella, responsable informatique de Troc de l'île. Le spécialiste du dépôt-vente (170 filiales et magasins franchisés à travers l'Europe) a déployé dans les quarante filiales de la société un système de sauvegarde en ligne (AGS-Backup). Auparavant, Troc de l'île réalisait la sauvegarde des données de ses magasins à l'aide d'un logiciel développé par son service informatique, qui permettait de copier les données automati-



Le spécialiste du dépôt-vente Troc de l'île a déployé dans les quarante filiales de la société un système de sauvegarde en ligne (AGS-Backup).

quement, chaque nuit, tout en gardant quinze jours un historique. Les responsables de magasin devaient charger des CD préformatés pour lancer la sauvegarde. Peu fiable, ce système imposait une tâche récurrente à des personnes n'ayant pas de compétences informatiques. Par ailleurs, le stockage en interne n'assurait aucune protection des données en cas d'incidents naturels ou de vol. D'autant que le parc informatique géré par Troc de l'île est d'une grande hétérogénéité (plus de 800 PC configurés sous différentes versions de Windows).  
Même approche chez Icade, filiale de la Caisse des dépôts et consignations, qui a pour objectif à l'horizon 2008 de structurer l'hébergement de ses sauvegardes nationales centralisées. Après avoir externalisé, dès 2000, une partie de ses activités sur un premier site en Ile-de-France, Icade a restructuré sa production dans le cadre d'un plan de services, et compte externaliser cette année les 50 % restants de ses applications liées à l'immobilier, la comptabilité et la bureautique de proximité (chez Interxion) dans un second site externe. À partir de 2008, un autre *datacenter* sera choisi afin de mettre en œuvre un plan de répartition et de gestion des risques. Le CIF (Crédit immobilier de France) a été confronté à une problématique liée à une réorgani-

sation de son SI passant d'une informatique régionale vers une informatique centralisée. Cet objectif induisait de multiples difficultés du fait d'une grande hétérogénéité des parcs et de l'absence de normes au niveau local. Il était par ailleurs important pour la direction de veiller à l'agencement au niveau global de certaines actions de sécurité pour les années à venir.

### Sécuriser le poste de travail

Le suivi du cœur de l'infrastructure était assuré, mais celui du poste client faisait défaut. Dans ce contexte, Éric Doyen, responsable de la sécurité du SI (RSSI) du CIF, prit conscience très tôt des risques croissants qu'encourait le poste de travail. Un premier état des lieux avait mis en exergue la globalité d'un nouveau phénomène, celui de l'apparition de nouveaux médias et périphériques gravitant autour du poste et que personne ne maîtrisait. Éric Doyen assure de manière transverse le management de la sécurité du SI, afin de garantir la conformité des normes établies *vis-à-vis* notamment le contrôle interne, ainsi que le suivi des risques opérationnels. Cette mission était jusque-là abordée sans outil spécifique au poste de travail. Ainsi, dans une démarche d'homogénéisation de son système et de centralisation de son organisation, le CIF a souhaité mettre en place un système de supervision de la sécurité des postes clients afin de gérer manière de manière uniforme ses postes clients et de contrôler la conformité de ses politiques de sécurité.

Répondre à ce besoin nécessitait un processus clair : d'une part, l'identification des éléments nécessaires au poste de travail, notamment en termes de périphériques externes, pour ensuite vérifier l'intégrité et la mise en conformité complète de ces postes afin d'homogénéiser ses systèmes et contrôler de manière régulière et globale ses politiques de sécurité interne. *"L'analyse de nos dernières statistiques nous montre que près de 50 % de l'activité du support provient d'incidents ayant pour origine le poste client. En parallèle, nous travaillons à mettre en place une politique de sécurité intelligente et proportionnée au sein de notre organisation désormais centralisée. Côté sécurité, nous nous attelons ainsi à mesurer la croissance de tous les nouveaux médias externes pour lesquels nous n'avons pas arrêté de décision en terme de politique"*, souligne Éric Doyen. ■

LOUIS ALLAIN

## UNE PLATE-FORME UNIQUE AU CRÉDIT AGRICOLE DU NORD

Une approche similaire a été mise en œuvre par le Crédit agricole du Nord (250 agences), qui a abandonné ses solutions précédentes (Infovista et Netview 6000) pour installer un outil (de ServicePilot Technologies, intégré par Nextiraone) dans le but de fédérer une gamme de services *via* une plate-forme unique : remontées d'alarmes en temps réel, supervision et analyse de l'ensemble du parc, historique des données, *reportings* personnalisés et prédéfinis, interconnexion avec d'autres outils de gestion interne et possibilité d'accès *via* un navigateur Internet depuis un poste standard.

En 2004, suite à la fusion de deux caisses régionales, le Crédit agricole du Nord avait décidé de refondre son réseau d'agences pour optimiser les coûts et accroître les débits en choisissant une nouvelle technologie de transport. Ce qui supposait que les besoins du *help-desk* soient pris en compte. Ce dernier devait en effet avoir une vision cartographique du réseau d'agences avec des remontées d'alarmes en temps réel. L'équipe administration réseau doit pouvoir collecter et analyser simplement les indicateurs clés du réseau Lan-Wan avec de la QoS (qualité de service). Cette équipe doit aussi pouvoir disposer d'un historique des données avec la possibilité d'activer ponctuellement un mode audit pour avoir un détail des flux transitant sur le réseau.