SÃ©curitÃ© Informatique : Pas de sÃ©curitÃ© sans PRA et PCA
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 30/9/2011 14:00:00

Traditionnellement, la sÃ©curitÃ© est abordÃ©e de maniÃ¨re assez classique et largement tournÃ©e vers une approche orientÃ©e **logiciel : anti spam, anti virusâ¦** Ces Ã©lÃ©ments sont bien entendu stratÃ©giques, mais **doivent Ãªtre complÃ©tÃ©s par des dispositifs plus structurants** affirme **Magdi Houry**, PrÃ©sident d'Euclyde.Â

Les aspects liÃ©s Ã lâinfrastructure sont donc cruciaux, notamment au niveau des data centers. Dans ce contexte, les notions de disponibilitÃ©, de connexion et de continuitÃ© de service sont Ã prendre en compte. Le plan de reprise dâactivitÃ© (PRA) et le plan de continuitÃ© dâactivitÃ© (PCA) sont des Ã©lÃ©ments clÃ©s de ce dispositif.

Mais de quoi parle-t-on ? Voici une courte dÃ©finition de ces Ã©lÃ©ments afin de mieux comprendre leurs champs dâapplication.

Le plan de reprise dâactivitÃ©, ou PRA (en anglais Disaster Recovery Plan ou DRP), permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activitÃ© d'une organisation.

Le plan de reprise d'activitÃ© doit permettre, en cas de sinistre, de basculer sur un systÃ¨me de relÃ¨ve capable de prendre en charge les besoins informatiques nÃ©cessaires Ã la survie de l'entreprise.

Il existe plusieurs niveaux de capacitÃ© de reprise ; le choix doit dÃ©pendre des besoins exprimÃ©s par l'entreprise. Un plan de reprise d'activitÃ© passe invariablement par une architecture multi sites, permettant au matÃ©riel sur le second site de ne pas Ãªtre affectÃ© par le sinistre.

Un plan de continuitÃ© d'activitÃ©, ou PCA, a pour but de garantir la survie de l'entreprise aprÃ¨s un sinistre important touchant le systÃ¨me informatique. Il s'agit de redÃ©marrer l'activitÃ© le plus rapidement possible avec le minimum de perte de donnÃ©es.

Ce plan est un des points essentiels de la politique de sÃ©curitÃ© informatique d'une entreprise.

A travers ces dÃ©finitions, lâon comprend bien que la prÃ©servation de lâactif IT est une prioritÃ© et quâil est nÃ©cessaire de bien mesurer la valeur des ses assets et donnÃ©es. Ainsi, selon le cabinet dâanalyse Markess, les domaines mÃ©tiers les plus concernÃ©s par des enjeux de continuitÃ© d'activitÃ© sont la messagerie ou encore les applications de finance et de production pour lâindustrie notamment.

Lâon remarque Ã©galement une Ã©volution vers les applications et infrastructures IP qui connaissent un bon dÃ©veloppement dans les entreprises. Globalement, il faut donc arriver Ã Ã©valuer Â« l'indisponibilitÃ© qui peut Ãªtre autorisÃ©e Â» et Ã dÃ©finir des prioritÃ©s, des techniques et un budget de mise en Åuvre et de fonctionnement.

Autre Ã©lÃ©ment, les PRA et PCA ne sont pas des chantiers dormants, ils doivent Ã©voluer de pair avec le systÃ¨me dâinformation et Ãªtre toujours en conditions opÃ©rationnelles. Dans ce contexte, il est nÃ©cessaire de mettre en place une politique de tests rÃ©guliers et de faire Ã©voluer son dispositif PCA-PRA.

Traditionnellement dÃ©ployÃ© dans des activitÃ©s imposant des contraintes rÃ¨glementaires le PRA- PCA nâest pas pour autant rÃ©servÃ© Ã ce type de sociÃ©tÃ©s.

Dans les faits, il sâadresse Ã toutes les entreprises souhaitant Ã la fois prÃ©server leur patrimoine numÃ©rique et assurer une continuitÃ© de service. On notera Ã©galement que la mise en Åuvre de ce mode de traitement permet Ã©galement de garantir une aide plus consÃ©quente vis-Ã -vis des assurances.

Les PRA et PCA sont donc un dispositif clÃ© de la sÃ©curitÃ© informatique et doivent faire partie de la stratÃ©gie sÃ©curitÃ© de lâentreprise dÃ¨s le lancement du systÃ¨me dâinformation. Avec la complexification des architectures rÃ©seaux et applicatives, il est fort probable que le PRA et le PCA se dÃ©veloppent Ã court terme.