La vulnÃ©rabilitÃ© des infrastructures IT : se prÃ©server de la cyber criminalitÃ©
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 9/5/2011 13:30:00

Incontestablement, **la cybercriminalitÃ© atteint un nouveau stade** et vient impacter toutes les formes organisationnelles et ce, quelle que soit leur taille. La derniÃ¨re **attaque du MinistÃ¨re des Finances** en est le parfait exemple.

Cela sâ□□explique principalement par la richesse du patrimoine numÃ©rique dont disposent les entreprises et par la dÃ©matÃ©rialisation croissante des procÃ©dures et actes de gestion (profession des avocats) . En effet, donnÃ©es clients, Ã©critures transactionnelles, brevets, informations stratÃ©giques se doivent dâ□□Ãªtre protÃ©gÃ©s de toutes attaques.

Nâ□□oublions pas que les entreprises peuvent Ãªtre responsables de leur continuitÃ© de service, de la confidentialitÃ© de leurs donnÃ©es et de celles qui leur sont confiÃ©es, etc. Une solide protection est donc nÃ©cessaire et Ã plusieurs niveaux : technique, organisationnel, assuranceâ□¦ Ainsi, comme les professions des experts comptables qui sont reconnus tiers de confiances.

Compte tenu de la nature de lâ□□activitÃ© , la pertinence du niveau de sÃ©curitÃ© pourra Ãªtre laissÃ©e Ã l'apprÃ©ciation lÃ©gislative. Ainsi, on peut considÃ©rer que le respect des best practices assorti d'un dÃ©lai de rÃ©action rapide viendront dÃ©montrer la bonne foi de la sociÃ©tÃ© et attester que cette derniÃ¨re a dÃ©ployÃ© tous les moyens nÃ©cessaires pour sÃ©curiser son systÃ¨me dâ□□information.

PrÃ©vention, conformitÃ© aux bonnes pratiques et rÃ©activitÃ© se positionnent de fait comme des obligations pour les TPE, PME et grands comptes. De maniÃ¨re synthÃ©tique, il est nÃ©cessaire de filtrer le trafic indÃ©sirable, de dÃ©tecter des anomalies, dâ□□alerter lâ□□entreprise en temps rÃ©el, dâ□□assurer sa responsabilitÃ© et de la prÃ©munir contre les ruptures dâ□□exploitation.

Â **Un premier travail consiste donc Ã auditer son infrastructure IT** avant de sâ□□Ã©quiper en matÃ©riel ou solutions de sÃ©curitÃ© non adaptÃ©es. Il sâ□□agit Ã©galement de sâ□□assurer quâ□□il nâ□□existe pas dâ□□erreurs de configuration dans les dispositifs existants. Il est donc nÃ©cessaire dâ□□identifier les vulnÃ©rabilitÃ©s avant de complÃ©ter les brÃ¨ches. Il sâ□□agit donc de sensibiliser lâ□□entreprise sur les risques.

Il est ensuite nÃ©cessaire de Â« filtrer Â» ou plutÃ´t de scanner en permanence lâ□□infrastructure IT. Nâ□□oublions pas que chaque jour les professionnels peuvent Ãªtre exposÃ©s Ã plusieurs centaines dâ□□attaques ! Il est donc utile dâ□□alerter lâ□□entreprise si son infrastructure manifeste des signes de vulnÃ©rabilitÃ© et de lui prÃ©coniser de rÃ©agir rapidement en mettant en Å□uvre tel ou tel nouveau dispositif ou en mettant Ã jour ces produits, par exemple. A ce niveau, lâ□□entreprise doit prendre des mesures informatiques Ã court terme pour ne pas Ãªtre impactÃ©e.

AprÃ¨s avoir menÃ© les actions mentionnÃ©es ci-dessus, il est ensuite fondamental dâ□□aborder un autre aspect souvent moins connu et pourtant nÃ©cessaire : la dimension Â« Assurance Â» qui, associÃ©e Ã la dimension informatique, permettra dâ□□avoir une approche 360Â° en matiÃ¨re de protection de son infrastructure et de ses donnÃ©es informatiques.

La responsabilitÃ© de l'entreprise est un facteur clÃ© Ã protÃ©ger. Lâ□□assurance est faite pour cela. Il sâ□□agit principalement de protÃ©ger et de pÃ©renniser lâ□□activitÃ© de lâ□□entreprise en lui permettant dâ□□accÃ©der Ã des garanties Ã valeur ajoutÃ©e portÃ©e sous lâ□□angle Â« Assurance Â». Cette couverture permet notamment de protÃ©ger lâ□□entreprise en cas de fuite des donnÃ©es, de rupture dâ□□exploitation, de contamination du SIâ□¦ Une couverture fournie par une assurance est donc particuliÃ¨rement importante et doit faire partie des plans de gouvernance des entreprises.

Au travers ces Ã©lÃ©ments il apparaÃ®t clairement que la protection doit Ãªtre multi-facette et ne pas se limiter au simple dÃ©ploiement de solutions de sÃ©curitÃ© qui ne suffisent pas nÃ©cessairement aux besoins des entreprises. Il convient de suivre un processus normalisÃ©, combinant analyse de lâ□□existant, surveillance en temps rÃ©el, adaptation des solutions et assurance.

[**Mikael Masson**, Directeur Risk Management et Cybercrime de Cyberprotect]