



INTERNET

Une toile à la merci des "interruptions d'infrastructure"

Le séisme survenu récemment au large de Taïwan et qui a privé d'Internet des millions de personnes en Asie a montré la vulnérabilité de la toile mondiale et seule une redondance systématique des infrastructures pourrait permettre d'éviter une paralysie totale, préviennent des spécialistes.

On ne sait pas bien se protéger contre les interruptions d'infrastructures", reconnaît Éric Domage, directeur sécurité Europe chez le groupe de conseil informatique IDC. Apparu au début des années 90, l'Internet est un vaste réseau informatique à l'échelle mondiale, reliant une multitude de sous-réseaux parlant un même langage de communication (IP, Internet Protocol), ce qui permet à des ordinateurs différents de communiquer entre eux. Cet immense maillage repose sur des infrastructures disséminées à travers le monde : routeurs "racines" (DNS), centres hébergeurs, serveurs et des milliards de petits re-routeurs permettant d'aiguiller le trafic sur les différents réseaux, via des câbles terrestres et sous-marins ou encore par voie satellitaire. Les incidents sont souvent mineurs. Comme en mars, lorsqu'une panne électrique avait affecté le fonctionnement de Redbus Interhouse, un important

centre hébergeur de la banlieue de Paris, perturbant le fonctionnement d'un grand nombre de sites pendant plusieurs jours. Mais l'un des points faibles de l'Internet, ce sont les "backbones", ces artères principales qui forment la "colonne vertébrale" de la toile et qui interconnectent l'ensemble des sous-réseaux et les continents entre eux. En Asie, une grande partie du trafic transitant via les câbles sous-marins endommagés, composés de gros faisceaux de fibre optique, a pu être "rerouté" in extremis vers d'autres serveurs aux États-Unis. Mais, avertit Éric Domage, "on est en zone de danger, car il y a une dépendance totale vis-à-vis des États-Unis".

Vers la redondance des liaisons électroniques

La seule solution, selon lui, réside dans la "redondance des liaisons électroniques", c'est-à-dire un doublement des infrastructures (câbles sous-marins ou routeurs), ainsi que la démultiplication des liaisons alternatives, notamment satellitaires. Aujourd'hui, 50 % du trafic mondial transite par le seul État de Virginie, où arrivent la plupart de terminaisons maritimes et où sont situés les principaux centres de routeurs "racines", qui permettent de transformer une adresse en lettres en adresse IP. Ces "routeurs racines" sont parti-

culièrement sensibles. "Un pirate ou une coupure de courant peut les mettre hors service et l'internaute n'a alors plus accès aux sites", explique Romain Levy, un des responsables du laboratoire d'expertise informatique Lexsi. D'autant qu'il n'en existe que quelques-uns dans le monde, principalement aux États-Unis, au Royaume-Uni et en Suède, note Emmanuel Sartorius, haut fonctionnaire de défense au ministère français de l'Économie. Un pays serait donc techniquement en mesure d'en "débrancher" un autre. Les conséquences d'une rupture des réseaux filaires, comme celle survenue en Asie, pourraient être limitées si l'on pouvait basculer les liaisons en mode sans fil, par satellite ou en Wimax (haut débit sans fil), fait-on remarquer également chez France Télécom. L'autre danger, c'est le "péril logique" : les attaques cybernétiques dirigées contre les infrastructures du Net. "Un pirate peut prendre le contrôle d'un routeur DNS et le faire tomber", explique Paulo Pinto, directeur du laboratoire de recherche en sécurité informatique Sysdream. "Si la redirection de secours ne fonctionne pas, un pirate peut très bien déconnecter un continent". ■