

Incidents télécoms en Europe : défaillances et attaques en hausse

En 2014, le secteur de la téléphonie fixe a concentré la plus grosse part (47%) des incidents rapportés par les autorités nationales de régulation des télécoms auprès de l'Enisa (European Union Agency for Network and Information Security). L'Agence européenne est chargée d'assurer la sécurité des réseaux de l'information à l'échelle européenne en facilitant les contacts entre les institutions et les entreprises. Elle se positionne en tant qu'expert en sécurité IT auprès des autorités nationales et des institutions européennes. Il propose des meilleures pratiques d'échange mais aussi des opérations de sensibilisation auprès des citoyens.

L'année dernière, pas moins de 137 incidents majeurs ont été rapportés par 24 pays de l'Union et un pays de l'Efta (European free trade association) parmi la Suisse, l'Islande, la Norvège et le Lichtenstein. Quatre pays de l'Union n'ont connu aucun incident majeure de sécurité, officiellement du moins, selon le [le rapport 2014](#) de l'Enisa qui se garde de préciser l'origine des déclarations pour éviter, probablement, de mettre les Etats membres dans l'embarras.

Le mobile moins impacté que le fixe

La téléphonie mobile a concentré, pour sa part, 39% des principaux soucis réseau rapportés. En conséquence, les services Internet fixes et mobiles ont à leur tour constitué 34% et 35% respectivement des incidents. Une situation inversée par rapport à 2013 et 2012 alors que les services mobiles concentraient l'essentiel des incidents (jusqu'à plus de 50 constatés pour la data mobile). Néanmoins, les utilisateurs mobiles sont bien les principales victimes des incidents de téléphonie et Internet à raison de 1,2 et 1,7 million de personnes affectées respectivement contre 300 000 et 400 000 pour les services fixes. Ce qui, en moyenne, se traduit par 13% des utilisateurs de l'Internet mobile concernés, 5% sur la voix en mobilité, 11% pour le même service sur les lignes fixes et 7% pour l'Internet depuis un accès résidentiel ou d'entreprise.

Cette somme d'incidents trouve dans une large majorité (66%) son origine dans les défaillances des systèmes et techniques généralement propres aux pannes de routeurs et commutateurs, et bug logiciel. Un ratio comparable d'une année sur l'autre. Dans 20%, l'incident a été causé par une erreur humaine, là encore un taux équivalent à celui de 2013. Les attaques informatiques sont en revanche en hausse à 9% et dépassent désormais les coupures de service provoquées par les catastrophes naturelles (5%). Notons que 16% des pannes systèmes sont dues à des défaillances tierces (comme les coupures d'électricité) et que dans 12% des cas, les incidents provenaient de problèmes d'interconnexion entre opérateurs.

Une erreur humaine : 3 millions d'utilisateurs sans

service

Mais ce sont les erreurs humaines qui ont affectés le plus d'utilisateurs. Plus de 3 millions de personnes en moyenne par incident ont subi des désagréments à cause d'une erreur de manipulation contre un peu plus d'1 million suite à une attaque malicieuse et 852 000 pour une défaillance matérielle. Les phénomènes naturels ont concernés moins de 220 000 personnes en 2014. Mais ces derniers affectent plus longtemps les services. En moyenne, ils bloquent le service 81 heures, contre 43 heures pour les pannes systèmes, 23 heures suite à une erreur humaine tandis que les attaques informatiques sont finalement vite appréhendées avec un impact de 12 heures en moyenne. Notons que cette moyenne de 81 heures constitue la durée record d'absence de service depuis que la publication en 2012 du premier rapport de l'Enisa. Une moyenne qui occulte néanmoins la durée maximale de 117 heures d'incident relevée haut la main par les changements de logiciel ou mise à jour. Modifier un environnement qui fonctionne est visiblement plus que jamais risqué.

Lire également

[Recrudescence d'attaques DDoS depuis de «vieux» routeurs](#)

[Une vulnérabilité enrôle massivement pour amplifier les attaques DDoS](#)

[Les protocoles Internet de plus en plus exploités par les attaques DDoS](#)

crédit photo © Andy Dean Fotolia.com