

25/01/2011

www.enisa.europa.eu

Identification des facteurs décisifs pour la conception des réseaux résilients de bout en bout

La résilience des réseaux de données est cruciale pour l'économie et la société. Pourtant, des trafics anormaux mais légitimes, des attaques malveillantes, des accidents ou erreurs humaines et des pannes techniques à des niveaux inférieurs peuvent toujours gêner l'accès aux réseaux. Cela a des conséquences majeures sur la société de l'information, puisque les réseaux sont présents partout, derrière l'énergie, l'eau, ou encore le commerce électronique; en d'autres termes, sur l'infrastructure d'information critique toute entière. L'ENISA présente aujourd'hui les principes de conception de la «résilience de bout en bout» dans un champ d'application élargi, e2e Resilience, dans son nouveau rapport (<http://www.enisa.europa.eu/act/res/technologies/e2e>); c'est-à-dire comment les réseaux permettront une connectivité, tout en se concentrant sur la qualité. L'approche de bout en bout (e2e) implique des aspects qui dépassent, tout en s'y ajoutant, la technologie pour les organismes de standardisation et les responsables politiques.

La résilience est nécessaire lorsque les opérateurs perdent le contrôle du déroulement des événements, c'est-à-dire lorsque les incidents rendent les procédures de réactions aux incidents inefficaces et déstabilisent la gestion. C'est pourquoi la gestion de la résilience doit prendre en compte tous les aspects: les utilisateurs finaux, le contexte dans lequel le système est utilisé, la technologie du système, la structure de l'organisation, sa capacité de résilience et, enfin, la capacité de la société dans laquelle le système opère.

Se concentrant sur les réseaux et les services publics, [le nouveau rapport complet](#) de l'Agence identifie les facteurs décisifs de la résilience de bout en bout. Il indique également aux organismes de standardisation et aux régulateurs comment activer et gérer la résilience de bout en bout. Le concept de résilience de bout en bout est élargi dans ce rapport, passant d'une liaison uniquement à la couche réseau, à une approche plus complète et donc différente dans cette étude unique. Ce champ d'action élargi de la résilience de bout en bout est obtenu par la combinaison planifiée de modes de prévention, de protection, de réaction et par des dispositifs de récupération, qu'ils soient techniques, organisationnels ou sociaux.

Le [Professeur Udo Helmbrecht, Directeur Exécutif de l'Agence](#), a déclaré:

«Ce rapport fournit les principes de la conception de réseaux capables de porter des trafics de bout en bout, ce qui est d'une grande utilité pour les régulateurs nationaux.»



25/01/2011

www.enisa.europa.eu

Dans le détail, le rapport stipule que la résilience de bout en bout doit:

- Répondre aux incidents causant aussi bien des impacts très mineurs qu'extrêmes
- Répondre aussi bien à des situations pouvant être traitées par l'intermédiaire de procédures quotidiennes de réaction aux incidents qu'à des crises trop complexes pour être traitées suivant un mode procédural au jour le jour

Le rapport fournit également les caractéristiques complètes d'un système résilient:

- Un système résilient est fiable
- Une infrastructure résiliente est dotée d'une forte disponibilité qui constitue un effet de toutes ses composantes
- Un système résilient doit pourvoir la continuité commerciale et la gestion de risques imprévus ou inattendus
- Un système résilient doit offrir un niveau de sécurité adéquat pour les informations transmises
- La résilience de bout en bout requiert la résilience de toutes les composantes de l'infrastructure

Le rapport identifie également les bonnes pratiques visant à achever la résilience et devant être utilisées par les organismes de standardisation et les responsables politiques.

Contexte politique: L'importance de la résilience est par exemple soulignée dans [l'Agenda numérique](#), point 2.2, qui met l'accent sur l'importance d'une interopérabilité efficace entre les produits et services de l'information, en vue d'établir une société et des normes véritablement numériques. Cela est également soutenu dans la [Déclaration de Grenade](#) par exemple.

[Cliquez ici pour consulter l'intégralité du rapport.](#)

Pour toute demande d'entretien, veuillez contacter: Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Portable: +30-6948-460143, ou Slawomir Gorniak, Expert, +30-6970015163, slawomir.gorniak@enisa.europa.eu

Veillez noter: traduction. La version anglaise est la seule version officielle.

