

27/08/2012

EPR010/2012

www.enisa.europa.eu

L'agence européenne ENISA révèle les lacunes de l'application de la législation sur la cybersécurité: les incidents ne sont pas détectés, voire non signalés

Dans un nouveau [rapport](#), l'agence européenne ENISA en charge de la sécurité informatique fait un bilan de la législation existante et future de l'Union Européenne concernant les mesures de sécurité et les déclarations d'incidents. L'analyse souligne des avancées importantes, mais identifie également des lacunes dans la mise en œuvre nationale des mesures, comme la plupart des incidents ne sont pas signalés.

Les incidents de cybersécurité ont un impact significatif sur la société. Voici cinq exemples bien connus:

- En 2012, [des millions de mots de passe de réseaux d'affaires](#) ont été exposés
- En 2011, [la tempête Dagmar](#) a détruit des millions de liaisons de communication scandinaves
- En 2011, [la défaillance d'un centre de données britannique](#) a interrompu des millions de communications d'affaires/d'entreprises dans le monde entier.
- En 2011, [un organisme de certification a été piraté](#), exposant ainsi les communications de millions d'utilisateurs
- En 2010, un fournisseur de télécommunications chinois [a détourné 15% du trafic Internet mondial](#) pendant 20 minutes

A chaque fois, des millions de citoyens et d'entreprises ont été gravement touchés. Mais la plupart des incidents ne sont pas signalés, voire même pas détectés. Le Dr Marnix Dekker et M. Chris Karsberg, les co-auteurs de ce rapport, affirment que: «*Les incidents informatiques sont le plus souvent tenus secrets lors de leur découverte, laissant les clients et les responsables politiques dans l'ignorance concernant la fréquence, l'impact et leurs causes profondes.*»

Le nouveau rapport "[Cyber Incident Reporting in the EU](#)" donne un aperçu de la législation existante et de celle à venir (voir le graphique ci-joint) concernant les clauses de déclaration obligatoire d'incidents de l'article 13a du paquet Télécom et de l'article 4 de la directive de confidentialité en ligne, l'article 15 pour le projet de régulation électronique de l'ID ainsi que les articles 30, 31, 32 de la réforme de la protection des données. L'étude montre des points communs et des différences entre les articles et se tourne vers l'avenir incarné par la stratégie européenne de sécurité en ligne. L'étude identifie également les points qui sont à améliorer. Par exemple, un seul des incidents mentionnés ci-dessus entrait dans le cadre du mandat des organismes de réglementation nationaux, ce qui indique qu'il existe des lacunes dans la réglementation. Ainsi, à l'échelle européenne, le partage des rapports d'incidents devrait être amélioré.

Beaucoup de progrès ont été accomplis récemment: Un groupe de travail de l'ENISA a développé pour les organismes de réglementation nationaux un socle commun de mesures de sécurité ainsi qu'un modèle de rapport d'incident. Cela permettra une mise en œuvre plus uniforme de l'article 13a. L'ENISA vient de recevoir des rapports sur les 51 incidents importants, envoyés par des organismes de réglementation et



27/08/2012

EPR010/2012

www.enisa.europa.eu

décrivant l'impact, les causes profondes, les mesures prises et les enseignements retenus lors de ces incidents. Ces outils seront utilisés comme une base de données pour la [stratégie européenne de sécurité informatique](#) et pour l' [Exercice européen de cyber-sécurité](#). Le directeur exécutif de l'ENISA, le [Professeur Udo Helmbrecht](#), a déclaré: "*Le signalement des incidents est essentiel pour obtenir une image réelle et concrète de la sécurité informatique. La stratégie européenne de cyber-sécurité est une étape importante et l'un de ses objectifs est d'étendre le concept de « rapports à disposition » telles que l'article 13a le stipule au-delà du secteur des télécommunications.*"

Sources: [European Cyber Security Strategy](#) et [Art 13a working group documents](#)

Pour plus d'informations: Ulf Bergstrom, Porte-parole de l'ENISA, press@enisa.europa.eu, Mobile: + 30 6948 460 143, ou Dr Marnix Dekker, ENISA, marnix.dekker@enisa.europa.eu

Veillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu

