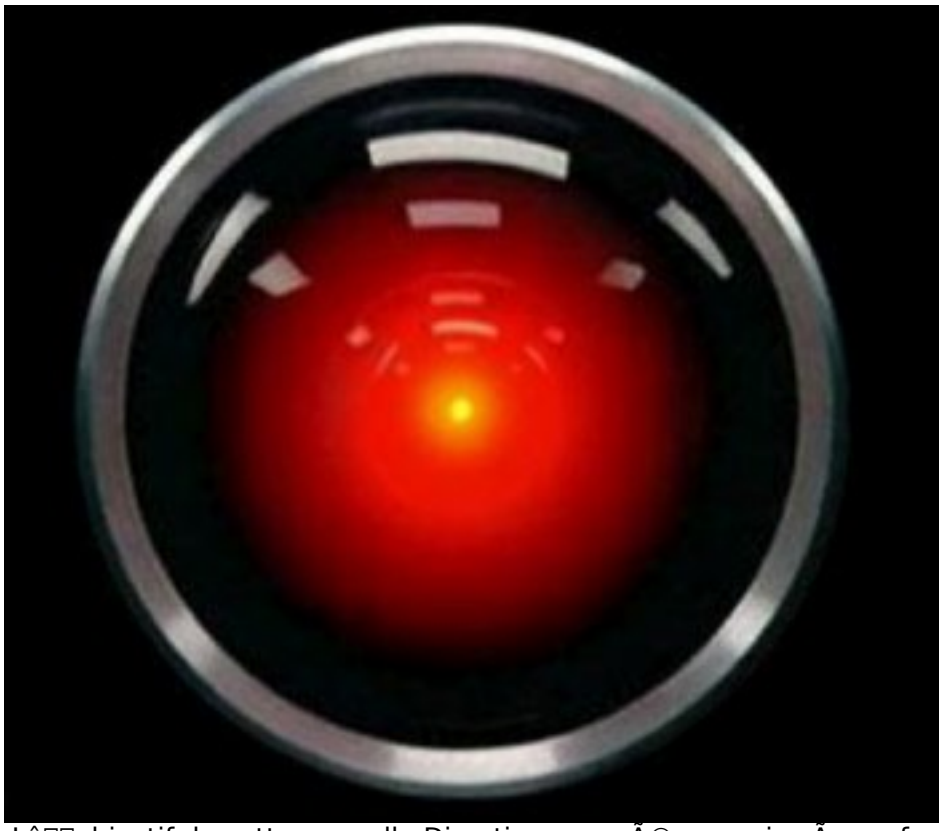
SÃ©curitÃ© : Vers une Union europÃ©enne de la SÃ©curitÃ© Informatique â¦
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 29/3/2013 14:00:00

Est-il temps dâinventer une Â« Ã©chelle de Richter Â» des incidents de sÃ©curitÃ©Â ?

Alors quâun projet de Directive a Ã©tÃ© prÃ©sentÃ© par **Neelie Kroes**, commissaire europÃ©enne chargÃ©e de la sociÃ©tÃ© numÃ©rique et au moment oÃ¹ le Conseil et le Parlement europÃ©ens doivent discuter de ce nouveau texte, voici un Ã©clairage sur ce projet de **FranÃ§ois Lavaste**, PrÃ©sident de NETASQ, acteur de la sÃ©curitÃ© informatique.



Lâobjectif de cette nouvelle Directive europÃ©enne vise Ã renforcer le niveau de sÃ©curitÃ© des systÃ¨mes dâinformation europÃ©ens et ce, de faÃ§on homogÃ¨ne. Au programme, la mise en place, dans chaque Ã©tat membre, dâune infrastructure complÃ¨te en matiÃ¨re de cybersÃ©curitÃ© et une obligation de notification des violations de la sÃ©curitÃ© des donnÃ©es personnelles sur 6 secteurs Â« cibles Â» qui sont les services financiers, les services Internet clÃ©s, lâÃ©nergie, la santÃ©, les transports et les administrations publiques.

Pour **FranÃ§ois Lavaste**, PrÃ©sident de NETASQ, si cette Directive va dans le bon sens, il reste maintenant Ã savoir comment elle se traduira concrÃ¨tement ? Et quelles en sont les limites Ã©ventuelles ?

Effectivement alors que lâon pouvait sâattendre, par exemple, Ã une obligation visant Ã inciter les Ã©diteurs de logiciels Ã Â« patcherÂ» les codes dÃ©fectueux, ou Ã des obligations pour les acteurs de la filiÃ¨res de mettre en place des mesures de prÃ©vention ou de sensibilisation en matiÃ¨re de sÃ©curitÃ© des donnÃ©es et des systÃ¨mes, le texte ne prÃ©voit, a priori, rien sur

ces sujets pour le moment.

En ce qui concerne la notification des violations, lâ□□idÃ©e est plutÃ´t bonne et incite Ã une vraie transparence et Ã une mise en commun europÃ©enne des efforts de sÃ©curitÃ©, toutefois, il faudra dÃ©finir clairement la terminologie Â« notification des incidents de sÃ©curitÃ© informatique Â» ?

Â« *Les Ã□tats membres veillent Ã ce que les administrations publiques et les acteurs du marchÃ© notifient Ã lâ□□autoritÃ© compÃ©tente les incidents qui ont un impact significatif sur la sÃ©curitÃ© des services essentiels quâ□□ils fournissent* Â»

Que recouvre exactement cette notion dâ□□incidents ayant â□□un impact significatifâ□□ sur la SSI ? Quelle Ã©chelle de gravitÃ© des incidents de sÃ©curitÃ© informatique devra Ãªtre utilisÃ©e ?

La sÃ©curitÃ© informatique est, de maniÃ¨re assez surprenante, un domaine qui nâ□□a pas encore inventÃ© ou imposÃ© son Â« Ã©chelle de Richter Â».

Il existe des indices de gravitÃ© pour les vulnÃ©rabilitÃ©s (faible, modÃ©rÃ©, important, critique) mais ceux-ci sont assez basiques. Certaines entreprises de sÃ©curitÃ©, inspirÃ©es probablement par les niveaux dâ□□alerte du plan VIGIPIRATE en France ou par ceux du NTAS (National Terrorism Advisory System) aux Etats-Unis, publient leur propre Ã©chelle de menace (basse, medium, Ã©levÃ©e, extrÃªme par exemple).

Ces indicateurs sont souvent subjectifs et prÃ©cÃ¨dent les incidents potentiels. Cependant aprÃ¨s un incident, aucune Â« Ã©chelle Â» de gravitÃ© nâ□□est vÃ©ritablement communÃ©ment admise et utilisÃ©e.

On pourrait imaginer quâ□□une telle Ã©chelle Â« a posteriori Â» de la gravitÃ© dâ□□un incident de sÃ©curitÃ© serait utile pour rapidement mettre en place, pour les victimes prÃ©venues, les mesures Ã prendre et pour que les mÃ©dias positionnent ces Ã©vÃ¨nements de maniÃ¨re la plus objective possible.