Séminaire CEPD - ENISA «Faire face aux failles de sécurité»
Parlement européen, Bruxelles, 23 octobre 2009

Remarques introductives

Peter Hustinx
Contrôleur européen de la protection des données

Mesdames et Messieurs,

J'ai le plaisir de vous accueillir à ce séminaire, organisé conjointement par le Contrôleur européen de la protection des données (CEPD) et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), avec le soutien généreux et hautement apprécié du Parlement européen.

Je voudrais en particulier souhaiter la bienvenue à M^{me} la Commissaire Viviane Reding, qui a accepté de prononcer un discours d'ouverture. La responsabilité politique du sujet d'aujourd'hui entre dans le cadre de vos compétences, mais votre participation active à cet événement souligne à la fois l'importance du sujet et votre engagement personnel à le traiter de manière correcte et efficace.

Je tiens également à souhaiter la bienvenue au D^{r} Udo Helmbrecht, qui vient d'entrer en fonction en qualité de directeur exécutif de l'ENISA. Veuillez accepter nos meilleurs vœux de réussite dans votre mission de développement de l'Agence, dans la perspective d'une coopération productive.

Pertinence des failles de sécurité

Les «atteintes à la sécurité» et la «notification des atteintes à la sécurité» ont, pendant un certain nombre d'années, constitué des concepts «éloignés», mais ce n'est plus le cas.

La presse fait état d'un nombre croissant de failles de sécurité, non seulement au Royaume-Uni, mais dans plusieurs autres États membres. En fait, il pourrait bien s'agir d'un problème structurel de la société d'information européenne. Nos activités quotidiennes dépendent de plus en plus de la bonne performance des technologies de l'information et de la communication. Elles sont numérisées en tant que données à caractère personnel et deviennent plus vulnérables.

Le développement de la législation en matière de failles de sécurité atteint désormais également l'Europe, comme l'atteste le réexamen de la directive 2002/58/CE (vie privée et communications électroniques). Outre une nouvelle obligation de notifier les atteintes, la Commission va également consulter l'ENISA, le groupe de l'article 29 et le CEPD au cours de l'élaboration des modalités techniques d'application.

Initialement, cette obligation s'appliquera uniquement au secteur des télécommunications et des fournisseurs de services internet, mais elle sera également pertinente dans un contexte plus large – à la fois en ligne et hors ligne – et sera dès lors également importante dans le contexte du réexamen de la directive 95/46/CE, s'inscrivant dans une tendance plus générale vers une meilleure gouvernance et une responsabilité accrue en matière de données.

Ainsi, augmentation de la pertinence et perspective horizontale sont autant de raisons pour le CEPD d'investir dans des actions préparatoires.

Ce séminaire est le deuxième d'un ensemble d'initiatives, la première manifestation ayant eu lieu en avril dernier. Organisée sous l'égide de l'initiative de Londres pour les Autorités de protection des données uniquement, elle jetait les bases d'un échange d'expériences et de meilleures pratiques. Toutefois, les résultats ont été pris en compte dans la préparation de ce séminaire et seront également utilisés dans le cadre de son suivi.

Structure du séminaire

Le séminaire est organisé en fonction du «cycle de vie» d'une faille de sécurité, à savoir, prévention, gestion, notification. La sélection de ces thèmes a pour objet de livrer un message clair aux responsables du traitement des données:

- Premièrement, renforcez les mesures de sécurité afin de protéger les données à caractère personnel. En outre, mettez en place les mécanismes appropriés pour démontrer que les mesures adéquates ont effectivement été mises en pratique.

- Deuxièmement, le risque/incident zéro est utopique, irréaliste. L'objectif est de fournir une certitude légale et technique à toutes les parties prenantes, du responsable du traitement des données au particulier, afin d'atténuer les risques pour les ramener à un niveau acceptable. Si une faille de sécurité se produit, assurez-vous que vous disposez des mécanismes nécessaires pour gérer et faire état de cette faille.

La gestion et la notification des failles de sécurité impliquent l'intervention de nombreux acteurs différents. Un dialogue bilatéral entre les responsables du traitement des données et les autorités chargées de la protection des données ne suffit pas. La responsabilité de chaque acteur doit être identifiée et prise en considération.

Ceci devrait être considéré comme un exercice de collaboration, dans lequel le niveau de sécurité engendré ne correspondra qu'au maillon le plus faible de cette chaîne d'acteurs (compagnie d'assurance, services chargés de l'application de la loi, responsables du traitement technique, autorités de certification, auditeurs, etc.).

Rôle du CEPD

Le CEPD a, et aura à l'avenir, un rôle à jouer en matière de supervision dans les failles de sécurité au sein des institutions de l'UE:

- Atteintes aux systèmes informatiques à grande échelle: deux notifications jusqu'à présent.

- La Commission européenne a introduit dans ses nouvelles modalités d'application relatives à la sécurité des systèmes d'information, l'obligation de notifier une faille de sécurité à son délégué à la protection des données.
- Le réexamen de la directive 2002/58 pourrait également entraîner celui du règlement n° 45/2001 et introduire une obligation globale de notification des incidents de sécurité.

Le CEPD a soutenu le réexamen de la directive 2002/58 et, avec le groupe de l'article 29, fournira des conseils sur les modalités de mise en œuvre et autres initiatives dans ce domaine.

Remarques complémentaires

La gestion et la notification des failles de sécurité constituent un phénomène relativement nouveau. Les piliers de la notification des atteintes à la sécurité sont en place, mais il reste un long chemin à parcourir pour l'ensemble des responsables du traitement des données, autorités chargées de la protection des données et autres parties prenantes.

Ce qui importe le plus à ce stade est de comprendre les interconnexions et de développer l'ensemble approprié de mesures afin d'assurer une stratégie efficace et des incitations adéquates pour renforcer la sécurité des données. Nous avons tous besoin d'apprendre à ce stade et, au sein de notre institution, nous espérons que la réunion de ce jour atteindra cet objectif.

Sur une note plus pratique, je voudrais vous rappeler que ce séminaire se déroule selon la règle «Chatham House», en vertu de laquelle les participants sont libres d'utiliser les informations reçues, mais ne doivent révéler ni l'identité, ni l'affiliation des intervenants, de même qu'ils ne doivent pas révéler l'identité des autres participants.

Deux orateurs n’ont pas été en mesure de confirmer leur participation. Un troisième orateur a eu des problèmes de dernière minute. Néanmoins, nous prévoyons une interaction animée au cours des trois séances de la journée.

J’invite à présent M^{me} la Commissaire Reding à prendre la parole pour son discours d’ouverture.