Les obligations légales de cybersécurité et de notification d'incidents

Colloque organisé par l'UNamur et le CCB

Vendredi 8 novembre 2019
Fondation Universitaire
Rue d'Egmont 11 - 1000 Bruxelles

La sécurité des données informatiques est devenue un enjeu majeur, non seulement pour garantir le respect du droit fondamental à la vie privée mais également afin de préserver la confiance de la population dans les réseaux, systèmes et produits ICT dont la fiabilité est essentielle à leur vie économique et sociétale. Vu le nombre d'intervenants, d'équipements et de processus impliqués dans les environnements numériques actuels, de nouvelles règlementations européennes – telles le RGPD, la directive NIS et le Cybersecurity Act – ont matérialisé cet enjeu. L'objectif de ce colloque est de faire passer le message que sécurité des données et accountability vont de pair : une obligation de moyens n'a de réelle puissance que lorsqu'elle est accompagnée de mesures permettant de vérifier si ses débiteurs ont été suffisamment prudents et diligents dans sa mise en œuvre.

Renseignements et inscriptions : www.crids.eu
sarah.fievet@unamur.be

Tarif : 200 € la journée (comprenant : l'ouvrage publié Chez Politeia, les pauses et le lunch).
Réduction de 25 % accordée aux étudiants, avocats stagiaires et 3 personnes de la même société y participant.

OBFG : 6 points

8h30 : Accueil et inscriptions
9h00 : Mot de bienvenue
- Miguel DE BRUYCKER, directeur du Centre pour la Cybersécurité Belgique (CCB)
- Alexandre DE STREEL, professeur à l'UNamur et directeur du CRIDS

9h20 : Introduction au phénomène de la cybersécurité et des réponses en Belgique
- Les risques cyber actuels et les actions du CCB – Phédra CLOUNER, directrice adjointe du CCB
- Cybersécurité et PME : votre entreprise est-elle prête ? – Laurie PHILIPS, responsable juridique et DPD adjoint au SPF Economie

1er volet : Les obligations de sécurité et de notification sous le régime du RGPD

9h50 : Données à caractère personnel, évaluation des risques, mesures de sécurité et notification d'incidents
- Franck DUMORTIER, chercheur au CRIDS et chargé de cours en droit de la cybersécurité

10h30 : Table ronde pratique sur les enjeux du RGPD en matière de cybersécurité
- Joëlle JOURET, Conseiller juridique au Comité Européen de la Protection des Données
- Philippe RAIDA, Conseiller en technologies et en sécurité de l'information à l'Autorité de protection des données
- Jean-Marc VANGYSEGHEM, DPD du Réseau Santé Bruxellois
- Violette DE NEEF, DPO aux Cliniques universitaires Saint-Luc

10h50 : ***Pause-café***

2ème volet : La certification sous le régime du Cybersecurity Act

11h10 : Les objectifs du Cybersecurity Act et des schémas de certification
- Manon KNOCKAERT, chercheuse au CRIDS

11h40 : Les normes internationales, l'accréditation et le Cybersecurity Act
- Maureen LOGGHE, directrice de BELAC (SPF Economie)
- Jean-Luc PEETERS, Information Security Expert au CCB

12h10 : ***Lunch***

3ème volet : Les obligation de sécurité et de notification sous le régime de la directive NIS

13h10 : Les opérateurs de services essentiels (OSE)
- Valéry VANDER GEETEN, responsable juridique et DPD du CCB
- Marion DARGENT, Information Security Expert au CCB
- Anne-Catherine GOYERS, juriste au CCB

14h00 : Les fournisseurs de services numériques (FSN)
- Benjamin DOCQUIR, avocat au barreau de Bruxelles (Osborne Clarke)

14h30 : La notification et la gestion d'un incident en pratique
- Pierre-Francois VANDENHAUTE, Conseiller ingénieur, Sécurité du Réseau IBPT
- Lionel FERETTE, Cybersecurity Analyst, CCB (Cert.be)

15h00 : ***Pause-café***

4ème volet : La journalisation, le ethical hacking et les méthodes d'enquête des autorités

15h20 : Cybersécurité, vie privée, imputabilité, journalisation et log files
- Franck DUMORTIER, chercheur au CRIDS et chargé de cours en droit de la cybersécurité

15h40 : Les politiques de divulgation coordonnée des vulnérabilités (hacking éthique)
- Valéry VANDER GEETEN, responsable juridique et DPD du CCB

16h00 : Cybersécurité et cybercriminalité : de l'enquête administrative à l'enquête pénale
- Catherine FORGET, chercheuse au CRIDS et avocate au barreau de Bruxelles (Jus Cogens)

16h30 : Comment collaborer avec des hackeurs éthiques d'une manière structurée et légale ?
- Stijn JANS, Fondateur de la plate-forme INTIGRITI (bug bounty)
- Jean-François SIMONS, CISO et DPO de BRUSSELS AIRLINES

17h00 : **Conclusions**