

## Maandag 10 Oktober 2016

Fondation Universitaire, Egmontstraat 11,  
1000 Brussel

De verplichtingen inzake informaticabeveiliging leiden tot veel discussies. Conform de richtlijnen 95/46/EU en 2002/85/EU – zoals omgezet in Belgisch recht bij de privacywet van 8 december 1992 en de wet van 13 juni 2005 betreffende de elektronische communicatie – dienen een groot aantal bedrijven hun informaticasystemen te beveiligen tegen cyberaanvallen. De inwerkingtreding van de nieuwe verordening “General Data Protection Regulation” (GDPR) en de richtlijn “Network Security and Information” (NIS) zou hun verplichtingen wijzigen.

Het eerste deel van deze conferentie zal worden besteed aan het materiaal, de juridische en technische inhoud van de verplichtingen inzake informatiebeveiliging die bedrijven moeten uitvoeren. Zal de nieuwe EU-regelgeving een hierop een impact hebben?

In het tweede deel van deze conferentie bespreken we de verplichtingen/mogelijkheden van bedrijven om inbreuken op de beveiliging van de gegevens en kwetsbaarheden te melden aan verschillende overheden. Moeten we, gezien de bestaande en toekomstige wetgeving, nadenken over het reguleren van "ethical hacking" en "responsible disclosure policies"? Hoe kunnen we botnets uitroeien met respect voor de privacy en regels omtrent gegevensbescherming? Zal het Belgische CERT, dat nu wordt geïntegreerd in het Centrum voor Cybersecurity (CCB), nog steeds in staat zijn om anoniem samen te werken met bedrijven? Welke is de mening van de Computer Crime Unit van de federale politie over de samenwerking met private actoren en met digitale klokkenluider?

### 9h00 Inschrijvingen

9h30 Welkom, Alexandre De Streel, professor van UNAMUR en directeur van CRIDS.

### Deel 1 : De informatiebeveiliging

09h50 De belangen van de bedrijven voor de cybersecurity, Nathalie Dewancker, Cyber Security Coalition.

10h15 De juridische verplichtingen inzake informatiebeveiliging, Franck Dumortier, Senior Onderzoeker bij CRIDS (UNamur).

10h40 De uitvoering van de verplichtingen inzake informatiebeveiliging (ISO 27xxx, security frameworks, etc), Daniel Letecheur, FEDICT.

11h05 De verplichtingen inzake informatiebeveiliging ten aanzien van de bedrijven. Jan Leonard, Data Protection Officer Orange Belgium en Emmanuel Bergmans, Internet System Engineer, I-Logs sprl.

11h30 Discussie met de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL) en de CCB.

### 12h00 Lunch

### Deel 2 : Inbreuken op de beveiliging van de gegevens en kwetsbaarheden, welke meldplicht?

13h00 Digitale klokkenluiders en preventieve maatregelen om digitale kwetsbaarheden te detecteren, Valery Vander Geeten, Legal attaché at the Centre for Cybersecurity (CCB).

13H25 Botnet eradication project, Bruno Schröder, Microsoft.

13H50 Cybersecurity maatregelen en privacy, Stefan Verschuere, Ondervoorzitter van CBPL.

14h15 Discussie met het Belgisch Instituut voor Postdiensten en Telecommunicatie.

### 14h50 Koffie

15h10 Medewerkingsverplichting van private actoren en overheden. Catherine Forget, Onderzoekster bij CRIDS en advocate.

15h35 Een aantal praktische gevallen van samenwerking tussen de private actoren en de overheden, Walter Coenraets, Federal Computer Crime Unit (FCCU).

16h00 Discussie met moderator, Franck Dumortier

16h25 Standpunt van de FOD Justice, Carl Bartier van de Dienst « Information security » en Alexander Hoefmans of Damien Moreau van de Dienst « Data protection ».

16h35 Standpunt van de FOD Economie, Alain Godfurnon

16h45 Conclusie, Alexandre De Streel.

### 17h00 Receptie.

Inlichtingen en inschrijvingen : [www.crids.eu](http://www.crids.eu)  
081/72.52.04 - [sarah.fievet@unamur.be](mailto:sarah.fievet@unamur.be)

Talen: drietalen (English/French/Dutch)

Tarief: 150 euros (met lunch)  
(Een publicatie van Anthémis zal gepubliceerd worden)

Reductie van 25 % voor de studenten, advocaat stagiair, en drie personen deelnemende van hetzelfde bedrijf.