

# Beveiliging in ICT

## een systematische aanpak

### Permanente Vorming

#### Module 0: Inleidende begrippen

13 en 20 januari 2005

#### Module 1: Concepten en organisatie van ICT-beveiliging

27 januari, 3 en 17 februari 2005

#### Module 2: Toepassingen van technische beveiliging

24 februari, 3, 10, 17 en 24 maart 2005

oefeningen: 19 maart 2005

#### Module 3: Fouttolerante informatiesystemen

21 en 28 april 2005

#### Module 4: Juridische aspecten

12 en 19 mei 2005

#### Module 5: Audit en controle van ICT-beveiliging

26 mei 2005

### Wetenschappelijke coördinatie

Prof. Dr. ir. Eric Laermans

Vakgroep Informatietechnologie, UGent, IBBT

Prof. Dr. ir. Piet Demeester

Vakgroep Informatietechnologie, UGent, IBBT

Prof. Dr. ir. Rik Van de Walle

Vakgroep Elektronica en Informatiesystemen, UGent, IBBT



Faculteit  
Bio-ingenieurswetenschappen

## Vormende waarde

Het doel van deze opleiding is de cursist te helpen bij het identificeren en het verhelpen van de risico's die de veiligheid van een ICT-infrastructuur bedreigen. Hij zal in staat zijn de technische mechanismen te begrijpen die bijdragen tot de gewenste beveiliging of die de schade van mogelijke inbreuken kunnen beperken. Hij zal ook inzicht krijgen in de juridische en organisatorische aspecten van ICT-beveiliging: welke implicaties heeft de wetgeving op een bedrijf en hoe implementeert en controleert men een beveiligingsbeleid?

## Getuigschrift van Permanente Vorming van de Universiteit Gent

De aanwezigheid tijdens de sessies en de evaluatie aan het einde van de opleiding bepaalt of de deelnemer slaagt. Elke deelnemer die modules 1 en 2, en minstens 1 van de modules 3 tot en met 5 bijwoont en hierover met succes examen aflegt, ontvangt een Getuigschrift van Permanente Vorming van de Universiteit Gent. Getuigschriften zijn een persoonlijke verdienste: deelnemers die een getuigschrift ambiëren kunnen zich niet laten vervangen, andere wel.

## Waarom dit programma?

Computers en communicatienetwerken zijn niet meer uit onze wereld weg te denken. Kritische onderdelen van het bedrijfsleven maken gebruik van ICT-infrastructuur, zodat we ons terecht de vraag moeten stellen hoe veilig deze infrastructuur wel is.

Geregeld verschijnen in de pers verhalen over inbreuken tegen deze beveiliging en de soms enorme economische schade die eruit voortvloeit. Het gaat dan over grootschalige aanvallen door nieuwe computervirussen die netwerken van grote bedrijven lam leggen, of over hackers die binnengedrongen zijn in het netwerk van een bankinstelling, of nog de gebrekkige beveiligingsinstellingen van de draadloze netwerken van een ziekenhuis. Naast de rechtstreekse schade van dergelijke incidenten (verloren gegevens, tijd, geld), is er mogelijk ook de negatieve impact op het imago van het bedrijf. Het is duidelijk dat beveiliging een zorg moet zijn voor elk bedrijf.

Beveiliging is reeds aan bod gekomen in andere opleidingen van het IVPV, maar deze opleiding bundelt de verschillende aspecten van ICT-beveiliging —technische, maar ook organisatorische en juridische— in één enkele opleiding.

## Doelpubliek

De doelgroep van deze opleiding bestaat vooral uit enigszins technisch geschoolden, maar niet noodzakelijk experts in ICT: de gebruikers van computers en netwerken, maar ook de beheerders van ICT-infrastructuur. Voor wie minder vertrouwd is met ICT is een inleidende module voorzien die de basiskennis meegeeft die nodig is om deze opleiding te kunnen volgen.

## Module 0: Inleidende begrippen

---

### Deel 1: Inleidende begrippen

De aanpak van deze opleiding is zeker niet overdreven wiskundig of technisch maar toch is een minimale kennis van de gebruikte technologieën vereist. Deze sessie is bedoeld voor wie een beperkte technische achtergrond heeft en/of niet helemaal vertrouwd (meer) is met de woordenschat en de basisconcepten van informatie- en communicatietechnologie. In deze les wordt de werking van computers, besturingssystemen en software kort toegelicht en wordt aangegeven waar de kwetsbare punten van dergelijke systemen kunnen liggen.

### Deel 2: Het internet

Het internet speelt een centrale rol bij de uitwisseling van informatie tussen gebruikers en informatiesystemen. Meteen zorgt dit ook voor een groot aantal beveiligingsproblemen die aan bod zullen komen in deze opleiding. Het is dan ook van groot belang dat er een basiskennis aanwezig is rond de werking van het internet en de bijhorende protocollen. In deze inleidende les wordt de werking van het internet toegelicht en worden een aantal belangrijke protocollen kort besproken. Een aantal beveiligingsproblemen die optreden worden geïdentificeerd.

**Lesgevers: Eric Laermans, Piet Demeester**

**Data: 13 en 20 januari 2005**

## Module 1: Concepten en organisatie van ICT-beveiliging

---

### Deel 1: Basisconcepten en –technieken in ICT-beveiliging

Wat bedoelt men nu precies met ICT-beveiliging? Welke functionaliteiten wil men ermee realiseren? Waarom is beveiliging nodig? Deze vragen worden in deze sessie beantwoord.

Er wordt een overzicht gegeven van de belangrijkste basisdoelstellingen van ICT-beveiliging zoals vertrouwelijkheid, authenticatie, data-integriteit, non-repudiatie, beschikbaarheid.

In een tweede sessie wordt uitgelegd welke technieken men kan gebruiken om de gewenste doelstellingen van ICT-beveiliging te halen. De basisprincipes van symmetrische (conventionele) encryptie en asymmetrische encryptie (met publieke sleutel) worden besproken, zonder in te gaan op de wiskundige details. Daarnaast komen ook hashfuncties, protocollen voor berichtauthenticatie en tijdstempels aan bod, en hoe ze kunnen gebruikt worden voor ICT-beveiliging. Verder wordt ingegaan op het beheer van sleutels die voor encryptie gebruikt worden, en de rol die certificaten en een public-key-infrastructuur (PKI) hierin kunnen spelen.

Naast deze traditionele technieken voor ICT-beveiliging komen ook biometrische technieken kort aan bod, wat hun voordelen, maar ook hun beperkingen zijn.

### Deel 2: Organisatie van ICT-beveiliging

In deze sessie wordt een praktijkgericht inzicht gegeven rond:

- de aanpak en componenten van een goed ICT-beveiligingsbeleid voor de gehele organisatie;
- een pragmatische aanpak rond uitwerking en installatie van een ICT-beveiligingsbeleid binnen een organisatie;
- hoe reageren op beveiligingsincidenten.

Tijdens deze sessie wordt een raamkader aangereikt rond de afstemming van ICT-beveiliging op de bedrijfsdoelstellingen met o.a. definiëring van rollen en verantwoordelijkheden, communicatiekanalen, aftoetsen van het beveiligingsbeleid binnen het juridisch kader.

Verder leert u hoe een beveiligingsprogramma uit te werken en te instal-

leren binnen dit beleid. Hier wordt, via een projectgedreven aanpak, aandacht gegeven aan het uitwerken van een dergelijk implementatieplan: planning, design, selectie, piloottrajecten, testen.

Tenslotte wordt aandacht geschonken aan de intelligente beheersing van beveiligingsincidenten binnen de organisatie: processen om dergelijke incidenten snel te detecteren, te identificeren en te analyseren plus procedures om te reageren (business contingency, disaster recovery) inclusief vereiste organisatie, escalatie, communicatie, opleiding, controle en het aanleggen van documentatie voor onderzoek.

**Lesgevers: Eric Laermans, Marc Vael**  
**Data: 27 januari, 3 en 17 februari 2005**

## Module 2: Toepassingen van technische beveiliging

In deze module geven we aan hoe de beveiligingstechnieken uit de eerste module kunnen gebruikt worden om de gewenste beveiliging te realiseren.

Deze beveiliging kan gebeuren op het niveau van de applicatie, zoals met een programma als PGP (Pretty Good Privacy), gemeenzaam gekend en gebruikt en tevens vrij toegankelijk. We zien hoe de toegang tot een systeem kan beschermd worden, niet alleen met het klassieke mechanisme van wachtwoorden, maar ook met technieken als Kerberos of een systeem op basis van X.509-certificaten. Verder behandelen we de elektronische documenten en hoe een klassieke handtekening te vervangen door een minstens even veilige digitale handtekening.

De beveiliging kan ook ingebakken zijn in het gebruikte communicatiesysteem: S/MIME, voor e-mail, TLS/SSL voor het WWW -, het IP-Security protocol bij VPN (Virtual Private Network). Er wordt ook aandacht besteed aan de ingebouwde beveiliging van draadloze netwerken als GSM en IEEE 802.11.

Het gebruik van cryptografische beveiligingstechnieken alleen is echter niet voldoende om de veiligheid van een computersysteem te garanderen. Geregeld duiken nieuwe computervirussen op die ervoor zorgen dat belangrijke sites of zelfs het hele internet ei zo na lamgelegd worden. We zien hoe dergelijke virussen, wormen en ander malware (malicious software) werken, hoe een (distributed) denial-of-service-aanval kan ontstaan, en welke verdedigingsmechanismen hiertegen bestaan: virusscanners, firewalls en intrusiedetectiesystemen.

Ook het aspect van fysische beveiliging wordt besproken. Bij een gestolen computer, behoorlijk beveiligd voor normaal gebruik in een netwerk, kunnen de erop opgeslagen data toch gelezen worden. Ook de mogelijkheden voor de opslag van geheime sleutels voor asymmetrische cryptografie, met aandacht voor smartcards en andere tokens komen aan bod, evenals het risico van signaalblokkering voor draadloze netwerken.

Enkele belangrijke technieken uit deze module zullen geïllustreerd worden in een demonstratiepracticum en in een afzonderlijke practicumssessie zal de cursist zelf ervaring kunnen opdoen in het gebruik van beveiligingsinstrumenten.

Deze module wordt afgerond met een sessie over de state-of-the-art en de trends in ICT-beveiliging. Zijn onze informatiesystemen in de laatste jaren veiliger geworden en wat kunnen we verwachten voor de nabije toekomst? Er wordt geprobeerd om een antwoord te geven op vragen als: Bieden de huidige cryptografische algoritmen een voldoende bescherming voor 20 jaar en meer? Zijn er alternatieven beschikbaar?

- Wat zijn de doelstellingen en implicaties van de nieuwe ontwikkelingen i.v.m. "trusted computing" (o.a. TCG, NGSCB van Microsoft, en TrustZone van ARM)?
- Wat zijn de risico's voor de bescherming van onze persoonlijke gegevens (privacy) en welke technologieën staan ter beschikking om deze risico's te reduceren?
- Zijn er technologische oplossingen voor het SPAM-probleem?
- Wat zijn de recente ontwikkelingen op het vlak van DRM (Digital Rights Management)?
- Hoe is het gesteld met de veiligheid van elektronische betalingssystemen en wat zijn de meest recente evoluties in dit domein?

Bijkomende onderwerpen kunnen toegevoegd worden naar aanleiding van actuele gebeurtenissen.

**Lesgevers: Eric Laermans, Bart Preneel**  
**Data: 24 februari, 3 en 10 maart, 17 en 24 maart 2005; oefeningen op zaterdagvoormiddag 19 maart 2005**

## Module 3: Fouttolerante informatiesystemen

### Deel 1: Fouttolerante netwerken

Er worden steeds strengere eisen gesteld aan de betrouwbaarheid van communicatienetwerken. In deze les wordt ingegaan op de typische fouten die optreden in communicatienetwerken (kabelbreuken, softwarefouten, brand, natuurrampen, ...) en hun impact op de volledige infrastructuur. Er wordt aangetoond hoe men dergelijke fouten kan verhelpen door protectie- en restauratiemechanismen en dit voor verschillende netwerktopologieën (ringnetwerken, vermaasde netwerken, hybride netwerken) en netwerktechnologieën (transportnetwerken, internet,...). Tevens wordt een analyse gemaakt van de kosten die fouttolerantie met zich meebrengt.

### Deel 2: Fouttolerante computersystemen

In deze sessie introduceren we hoe de configuratie van ICT-systemen een hoge beschikbaarheid of een hoge betrouwbaarheid kan garanderen. Enerzijds laat hardwareredundantie toe om de systemen te laten voortwerken ondanks de uitval van componenten (standby- en TMR-architecturen). Anderzijds kan informatieredundantie instaan voor de integriteit van de data (codes, RAID, back-upstrategieën). Met verschillende industriële voorbeelden illustreren we hoe de opgeslagen gegevens en de rekencapaciteit beschermd kunnen worden tegen stroomuitval, defecte componenten en andere calamiteiten, en hoe dit past in het bredere kader van disaster recovery.

**Lesgevers: Mario Pickavet, Geert Deconinck**  
**Data: 21 en 28 april 2005**

## Module 4: Juridische aspecten

### Deel 1: Digital Rights Management (DRM)

Digital Rights Management (DRM) is een hot topic binnen het domein van ICT/multimedia-toepassingen. Platenmaatschappijen voeren al verschillende jaren een verbeterde strijd om de illegale verspreiding van digitale muziek (onder meer mp3-bestanden) tegen te gaan. Denk maar aan recente ophefmakende rechtszaken tegen Napster of KaZaA.

DRM laat toe om rechten ten aanzien van digitale items te beheren. Voorbeelden van digitale items: muziekbestanden; digitale beelden of video's; software-programma's; enz., voorbeelden van 'rechten': het recht om digitale items af te spelen; het recht om deze items te kopiëren; enz.

Ontwikkelaars van DRM-tools geloven dat deze tools de illegale verspreiding (of de illegale consumptie) van digitale items zal kunnen stoppen, anderen geloven dat hackers altijd een stapje voor zullen zijn en dat DRM-tools de verwachtingen nooit zullen kunnen inlossen.

Tijdens deze sessie wordt een overzicht gegeven van enkele technologieën die aan de basis liggen van DRM: vocabularia en talen die in staat zijn om rechten ten aanzien van digitale items uit te drukken (zgn. 'Rights Data Dictionaries' en 'Rights Expression Languages'); technieken voor het beheer en de bescherming van intellectuele eigendom (IPMP systems - Intellectual Property Management and Protection); beveiligingstechnieken op het niveau van de digitale items zelf (o.a. 'watermarking' en 'scrambling'); enz. Daarnaast worden, ter illustratie enkele concrete DRM-systemen besproken.

### Case: Beveiligingsaspecten van betalingen met chipkaarten

Steeds meer organisaties hebben geïnvesteerd of plannen investeringen in chip-gebaseerde infrastructuur voor betalingen met krediet- en debetkaarten. Banken die chipkaarten verdelen aan hun klanten zullen zich beter kunnen verdedigen tegen fraude en tegelijk kunnen profiteren van globale interoperabiliteit door de EMV-(Europay-MasterCard-Visa)-ICC-specificaties te gebruiken.

Deze sessie geeft een overzicht van de beveiligingsaspecten van deze betalingsmethodes en onderstreept de mogelijkheden voor risicobeheer die chipkaarten aan de banken bieden. Ze zal ook inzicht verschaffen in de nodige ondersteunende beveiligingsdiensten, zoals sleutelbeheer en beveiligingscertificatie. Tenslotte zal deze voordracht de nieuwe tendenzen behandelen, zoals multi-toepassingskaarten, e- en m-commerce.

## Deel 2: Wettelijke implicaties

Bij ICT-beveiliging mogen juridische aspecten niet over het hoofd gezien worden. ICT-beveiliging wordt soms door de wet expliciet verplicht gesteld, bijvoorbeeld voor de verwerking van persoonsgegevens of voor operatoren en dienstenaanbieders op openbare communicatienetwerken. Anderzijds zijn er bij het organiseren van ICT-beveiliging ook juridische beperkingen. Bij het registreren van e-mailverkeer van werknemers in ondernemingen of van gebruikers op openbare netwerken, moet men rekening houden met regels inzake de bescherming van de persoonlijke levenssfeer. Voor het gebruik en de export van cryptografie gelden eveneens bepaalde regels en ook de Amerikaanse wetgeving op de rapportering van beursgenoteerde bedrijven (Sarbanes-Oxley Act) vereist de nodige informatiebeveiliging om de correctheid van de verstrekte financiële informatie te garanderen.

Bepaalde beveiligingstechnieken hebben specifieke juridische gevolgen, bijv. de elektronische handtekening, die binnen afzienbare tijd door elke bezitter van een Belgische elektronische identiteitskaart kan worden gecreëerd. Er is ook een juridisch kader uitgetekend voor sommige aanbieders van diensten die met beveiliging te maken hebben, zoals certificatieautoriteiten.

Tenslotte wordt ook aandacht besteed aan het doorbreken van beveiligingsmaatregelen. Sommige activiteiten, zoals inbraak in informatiesystemen of het verspreiden van virussen, kunnen bestraft worden als strafrechtelijke misdrijven maar voor andere activiteiten zoals "wardriving" of "portscanning" zijn er wat meer twijfels. Speciale regels gelden voor het doorbreken van technische beveiligingsmechanismen in het kader van "digital rights management"

**Lesgevers: Rik Van de Walle, Marijke De Soete, Jos Dumortier**

**Data: 12 en 19 mei 2005**

## Module 5: Audit en Controle van ICT-beveiliging

In deze sessie wordt een praktijkgericht inzicht gegeven rond:

- de aanpak en componenten van een goede controle rond het beveiligingsbeleid binnen de gehele organisatie;
- hoe de resultaten van dergelijke audits en controles te presenteren en aan wie?

Een vitaal onderdeel, nl. hoe een beveiligingsprogramma controleren binnen vooropgestelde normen en afspraken rond informatiebeveiliging, wordt belicht. Ook hier wordt het belang van een goede regelmatige rapportering op basis van meetbare elementen aangetoond met aandacht voor de vertaling naar operationele taken en verantwoordelijkheden, kosten/baten van monitoring, certificering en regelmatige compliance-audits rond fysieke, administratieve en technische controles (inclusief behandeling van non-compliance elementen), meten en opvolgen en rapporteren van effectiviteit en efficiëntie van beveiligingscontroles, beveiligingsbewustzijn van alle betrokkenen op peil houden, opvolging en bijsturing van externe beveiligingsspecialisten (SLA's).

### Extra studiemateriaal via afstandsleren voor alle ingeschrevenen: Wiskundige grondslagen van encryptie

De opleiding bespreekt encryptie zonder veel aandacht voor de onderliggende wiskunde. De bedoeling van dit extra studiemateriaal is de geïnteresseerde cursist iets meer technische uitleg te geven over de precieze werking van de algoritmen die voor encryptie gebruikt worden. De algoritmen die hier aan bod komen zijn enkele courant gebruikte conventionele encryptiealgoritmen, zoals DES (en het eruit afgeleide 3DES) en zijn opvolger AES. Ook het asymmetrische encryptiealgoritme RSA en een hashalgoritme zoals SHA-1 worden besproken. Waar nodig, gaan we in op de gebruikte discrete wiskunde: bij voorbeeld priemgetallen en modulorekenen voor RSA. Tenslotte geven we een korte bespreking van modernere encryptietechnieken (zoals algoritmen met publieke sleutel gebaseerd op elliptische curven) en mogelijke technieken om cryptografische beveiliging te proberen kraken. Deze les wordt aan alle cursisten aangeboden op cd-rom met streaming video.

**Doelpubliek: geïnteresseerden in wiskundige achtergrond van encryptie. Lesgever: Eric Laermans**

## Deelnemings- en inlichtingsformulier

*Deze gegevens blijven strikt binnen het IVPV*

**Terug te sturen ten laatste 1 week vóór aanvang van de eerste module die u wenst te volgen.**

Naam: \_\_\_\_\_  M  V

Voornaam: \_\_\_\_\_

Functie: \_\_\_\_\_

Onderneming: \_\_\_\_\_

Adres: \_\_\_\_\_

Telefoon: \_\_\_\_\_ Fax: \_\_\_\_\_

E-mail: \_\_\_\_\_

Sector: \_\_\_\_\_ Aantal personeelsleden: \_\_\_\_\_

Privé-adres: \_\_\_\_\_

### Ik schrijf in voor de opleiding 'Beveiliging in ICT'

- Module 0: (enkel te volgen in combinatie met minstens 1 andere module)
- Module 1  Module 2  Module 3
- Module 4  Module 5
- Modules 0 t.e.m. 5  Modules 1 t.e.m. 5
- Ik bestel het handboek
  
- Ik wens het bijbehorend Getuigschrift van de Universiteit Gent te behalen.
- Ik betaal . . . . . € d.m.v. opleidingscheques werkgevers
- Ik betaal . . . . . € d.m.v. opleidingscheques werknemers
- Informeer mij over andere opleidingen van het IVPV

### Facturatie-adres

Naam: \_\_\_\_\_

Adres: \_\_\_\_\_

BTW nr.: \_\_\_\_\_

Datum: \_\_\_\_\_ Handtekening: \_\_\_\_\_

Een belangrijk referentiepunt voor deze sessie is CobiT (Control Objectives for Information and related Technologies) als een standaard die de goede praktijken beschrijft in beheer, controle en beveiliging van informatie en informatietechnologie.

**Lesgever: Marc Vael, Datum: 26 mei 2005**

## De lesgevers



### **Eric Laermans**

Universiteit Gent, Vakgroep Informatie-technologie, IBBT  
opleidingscoördinator



### **Piet Demeester**

Universiteit Gent, Vakgroep Informatie-technologie, IBBT  
opleidingscoördinator



### **Rik Van de Walle**

Universiteit Gent, Vakgroep Elektronica en Informatiesystemen, IBBT  
opleidingscoördinator

### **Geert Deconinck**

Departement Elektrotechniek (ESAT), KULeuven

### **Marijke De Soete**

Security4Biz, Brugge

### **Jos Dumortier**

Interdisciplinair Centrum voor Recht en Informatica, KULeuven, IBBT

### **Mario Pickavet**

Vakgroep Informatietechnologie, Universiteit Gent, IBBT

### **Bart Preneel**

Departement Elektrotechniek (ESAT), KULeuven, IBBT

### **Marc Vael**

Support Services, KPMG, Brussel

Frankeren  
als brief

Universiteit Gent

Instituut voor Permanente Vorming

T.a.v. Els Van Lierde

Technologiepark 913

9052 Gent - Zwijnaarde



Het IBBT, het Interdisciplinair instituut voor BreedBandTechnologie, is een onderzoeksinstituut opgericht door de Vlaamse regering, gericht op de Informatie- en Communicatie-Technologie (ICT) in het algemeen, en de ontwikkeling van breedbandtoepassingen in het bijzonder.

Meer info op: <http://www.ibbt.be>

## Praktische inlichtingen

Elke module kan apart gevolgd worden, behalve module 0.

De lessen vinden plaats aan de Universiteit Gent, Instituut voor Permanente Vorming, Gebouw Magnel, Technologiepark 904, 9052 Zwijnaarde op donderdagavond van 18u tot 21u30, in twee lessen, gescheiden door een broodjesmaaltijd. De praktijklessen vinden plaats op zaterdagmorgen tussen 9 en 12u.

## Deelnemingsprijs

De deelnemingsprijs omvat lesgeld, cursusnota's, frisdranken, koffie en broodjes. Betaling geschiedt na ontvangst van de factuur. Alle facturen zijn contant betaalbaar dertig dagen na dagtekening. Alle vermelde bedragen zijn vrij van BTW.

Mod. 0 (2 avonden): € 280

Mod. 1 (3 avonden): € 440

Mod. 2 (5 avonden + 1 voormiddag): € 880

Mod. 3 (2 avonden): € 280

Mod. 4 (2 avonden): € 280

Mod. 5 (1 avond): € 160

Modules 0 t.e.m. 5(reductie): € 1.880

Modules 1 t.e.m. 5(reductie): € 1.640

Handboek: "Cryptography and Network Security, Principles and Practices" van William STALLINGS, 3rd ed., intl. ed., Prentice Hall, Pearson Education, NJ (USA), 2003: € 58,50

**Indien minstens één deelnemer van een bedrijf inschrijft voor de volledige opleiding Beveiliging in ICT(modules 0/1 t.e.m. 5 of 1 t.e.m. 5), wordt voor alle bijkomende gelijktijdige inschrijvingen van hetzelfde bedrijf, per module of volledig pakket, een korting van 20% verleend. Facturatie geschiedt dan d.m.v. een gezamenlijke factuur.**

Inschrijving gebeurt door terugzending van het aangehecht deelnemingsformulier of via de IVPV-website.

**Bijzondere prijzen personeelsleden van UGent of geassocieerde hogescholen (consulteer de website vanuit deze instellingen).**

## Annulering

Annulering is mogelijk onder de volgende voorwaarden:

- gelieve steeds schriftelijk te bevestigen (per brief, fax of e-mail)
- bij annulering van de inschrijving 10 dagen of meer vóór de aanvang van het programma is een vergoeding verschuldigd van 25% van de deelnemingsprijs
- bij annulering minder dan 10 dagen vóór de aanvang van het programma is de volledige deelnemingsprijs verschuldigd.

## Inlichtingen

Bijkomende inlichtingen krijgt u op het secretariaat:  
Universiteit Gent, Instituut voor Permanente Vorming  
Els Van Lierde  
Technologiepark 913  
9052 Zwijnaarde  
Tel.: +32 9 264 55 82  
Fax: +32 9 264 56 05  
E-mail: [ivpv@UGent.be](mailto:ivpv@UGent.be)  
<http://www.ivpv.UGent.be/ictbeveiliging>

De Universiteit Gent is erkend als opleidingsverstrekker in het kader van de opleidingscheques van het Vlaams Gewest. Voor meer informatie en bestelling van de opleidingscheques zie [www.vlaanderen.be/opleidingscheques](http://www.vlaanderen.be/opleidingscheques)

Data onder voorbehoud van wijzigingen om onvoorziene redenen.

Indien u deze folder meerdere malen mocht ontvangen, dan verzoeken wij u vriendelijk deze aan uw collega's te bezorgen en ons dit te melden via e-mail.

**Bezoek onze website <http://www.ivpv.UGent.be>**

**voor andere opleidingen zoals:**

> **ICT voor managers**

> **Postacademische opleiding in expertisetechnieken**

> **Praktijkgerichte statistiek**

> **Industriële Automatisering**

> **Logistiek en mobiliteit in beweging, ...**