



Stichting NIOC en de NIOC kennisbank

Stichting NIOC (www.nioc.nl) stelt zich conform zijn statuten tot doel: het realiseren van congressen over informatica onderwijs en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin des woords.

De stichting NIOC neemt de archivering van de resultaten van de congressen voor zijn rekening. De website www.nioc.nl ontsluit onder "Eerdere congressen" de gearchiveerde websites van eerdere congressen. De vele afzonderlijke congresbijdragen zijn opgenomen in een kennisbank die via dezelfde website onder "NIOC kennisbank" ontsloten wordt.

Op dit moment bevat de NIOC kennisbank alle bijdragen, incl. die van het laatste congres (NIOC2023, gehouden op donderdag 30 maart 2023 jl. en georganiseerd door NHL Stenden Hogeschool). Bij elkaar bijna 1500 bijdragen!

We roepen je op, na het lezen van het document dat door jou is gedownload, de auteur(s) feedback te geven. Dit kan door je te registreren als gebruiker van de NIOC kennisbank. Na registratie krijg je bericht hoe in te loggen op de NIOC kennisbank.

Het eerstvolgende NIOC vindt plaats op donderdag 27 maart 2025 in Zwolle en wordt dan georganiseerd door Hogeschool Windesheim. Kijk op www.nioc2025.nl voor meer informatie.

Wil je op de hoogte blijven van de ontwikkeling rond Stichting NIOC en de NIOC kennisbank, schrijf je dan in op de nieuwsbrief via

www.nioc.nl/nioc-kennisbank/aanmelden_nieuwsbrief

Reacties over de NIOC kennisbank en de inhoud daarvan kun je richten aan de beheerder:

R. Smedinga kennisbank@nioc.nl.

Vermeld bij reacties jouw naam en telefoonnummer voor nader contact.



Risicofactor Mens bij Informatiebeveiliging

NIOC 2007 - drs. Stephen E. Querido BBA

DE HAAGSE
HOGESCHOOL
ACADEMIE VOOR ICT & MEDIA
ZOETERMEER



NIOOC ONTMOETINGSPLAATS VOOR ICT-ONDERWIJS

NIOOC	Programma	Aanmelden	Hotels	Sponsoring	Impressies	Interactief
Visie	Bestuur	Programmacommissie		Organisatiecommissie		Samenwerkingspartners

Congres NIOOC
17 & 18 april 2007
Amsterdam

Congressecretariaat
Oranje Nassaulaan 49
1075 AK Amsterdam
T 020 535 68 94
F 020 535 68 97
E congres2007@nioc.nl



*U kunt zich nog tot en met 12 april (12.00 uur!) inschrijven.
Daarna is inschrijving alléén op de congresdagen zelf mogelijk.*

Aanmelden NIOOC 2007

Nationaal Informatica Onderwijs Congres - NIOOC

De samenleving kan niet zonder goed opgeleide ict'ers. Het NIOOC wil stimuleren dat kennis in de volle breedte wordt benut. Eens in de twee jaar pakken we groots uit met een congres waar mensen uit het ict-onderwijs en het bedrijfsleven elkaar kunnen ontmoeten. Met een aantrekkelijk programma en unieke locaties is NIOOC 2007 wederom de ontmoetingsplaats waar u al uw collega's uit het **vo, mbo, hbo, wo en bedrijfsopleidingen** kunt treffen.

Programma 17 & 18 april



NIOOC ONTMOETINGSPLAATS VOOR ICT-ONDERWIJS

NIOOC	Programma	Aanmelden	Hotels	Sponsoring	Impressies	Interactief
Visie	Bestuur	Programmacommissie		Organisatiecommissie		Samenwerkingspartners

Congres NIOOC
17 & 18 april 2007
Amsterdam

Een onbekende ActiveX probeert uw systeem binnen te dringen. Voor blokkeren, [klik hier](#).

McAfee

U kunt zich nog tot en met 12 april (12.00 uur) inschrijven.

Congressecretariaat
Oranje Nassaulaan 49
1075 AK Amsterdam
T 020 535 68 94
F 020 535 68 97
E congres2007@nioc.nl



Nationaal Informatica Onderwijs Congres - NIOOC

De samenleving kan niet zonder goed opgeleide ict'ers. Het NIOOC wil stimuleren dat kennis in de volle breedte wordt benut. Eens in de twee jaar pakken we groots uit met een congres waar mensen uit het ict-onderwijs en het bedrijfsleven elkaar kunnen ontmoeten. Met een aantrekkelijk programma en unieke locaties is NIOOC 2007 wederom de ontmoetingsplaats waar u al uw collega's uit het **vo, mbo, hbo, wo en bedrijfsopleidingen** kunt treffen.

Programma 17 & 18 april

Risicofactor Mens bij Informatiebeveiliging

- Zijn er binnen uw organisatie duidelijke richtlijnen of regels met betrekking tot gevoelige of vertrouwelijke informatie?
 - Staan er sancties op het niet-naleven hiervan?
- Hoe kijkt u hier tegenaan: “Door een mislukte software update was het kassasysteem van Shell een aantal uren niet beschikbaar.”
- Heeft u (al dan niet toegestaan) een setje speakers aangesloten op uw werkplek-PC?



Risicofactor Mens bij Informatiebeveiliging

- Welke rol speelt (digitale) informatie in ons huidige leven?
 - **kennis:** wat is er op tv, hoeveel kost Digitenne, waar zit in deze buurt een afhaal-Fransoos, welke tram komt bij het Amstel Station, hoe sta ik geregistreerd bij McAfee, etc.
 - **argumenten:** u kunt beter geen melkproducten opwarmen in de magnetron, omdat uit onderzoek is gebleken dat ...
 - **actie:** hier kunt u uitrekenen hoeveel u op jaarbasis aan energie bespaart door spaarlampen te gebruiken. [Klik hier om in contact te komen met deze makelaar.](#)



Risicofactor Mens bij Informatiebeveiliging

- Informatie is macht! Informatie = €
- We gaan het niet hebben over: hackers, krakers, spammers, phishers, paardenfokkers uit Troje, virusliteratoren, etc.
- We gaan het wel hebben over u en ik; mensen met goede bedoelingen die door handelen of het nalaten daarvan inbreuk op beveiliging van informatie kunnen veroorzaken.



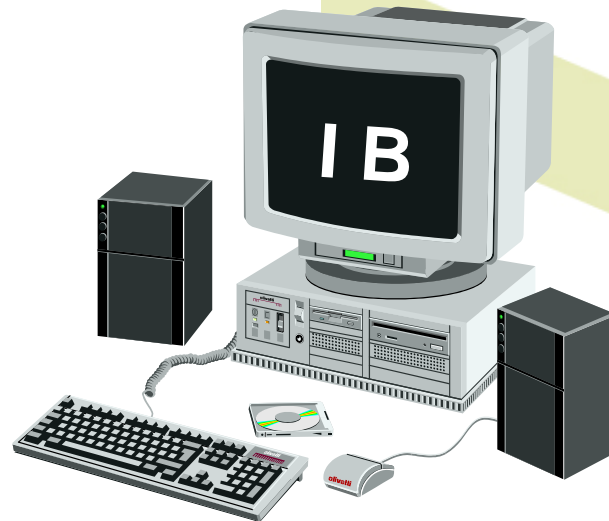
Risicofactor Mens bij Informatiebeveiliging

- Waardoor is er in ca. 80% van de incidenten bij IB sprake van menselijk falen?
- Soms wordt er een duidelijk te herleiden fout gemaakt; soms is het een keten van op zich weinig ernstige fouten met grote gevolgen.
- Het gaat bij IB niet alleen om waarborgen van integriteit en bescherming van informatie, maar ook om het veilig stellen van de beschikbaarheid van het informatiesysteem.



Risicofactor Mens bij Informatiebeveiliging

- Wat we met informatie doen is persoons-, rol- en contextgebonden:
 - Ter **kennisgeving** aannemen (hoofd)
 - Verwerpen (hoofd)
 - Verwerken (hoofd en gedrag)
 - Aanpassen (hoofd en gedrag)
 - Verstrekken (gedrag)
 - Verwijderen (gedrag)
 - Handelen (gedrag)
 - ...



Risicofactor Mens bij Informatiebeveiliging



- Wat maakt dat rol en context kunnen leiden tot verschillend gedrag?
 - Aan- of afwezigheid van significante anderen
 - Formele verantwoordelijk- en bevoegdheden
 - Rol-, taakopvattingen en integriteit
 - Verwachtingen \ ervaringen
 - Persoonlijkheid
 - (Bedrijfs-)cultuur
 - ...

Risicofactor Mens bij Informatiebeveiliging

- Aan- of afwezigheid van **significante** anderen
 - Positieve invloed van aanwezigheid van significante anderen*
 - Negatieve invloed van aanwezigheid van significante anderen
 - Positieve invloed van afwezigheid van significante anderen
 - Negatieve invloed van afwezigheid van significante anderen
- Motivatie (controle, opbrengsten)
- Sociale vergelijking (Festinger)



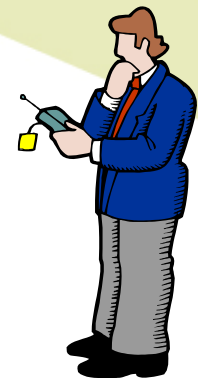
Risicofactor Mens bij Informatiebeveiliging

- Formele verantwoordelijk- en bevoegdheden:
 - Wat ik wel en niet mag doen
 - De mate waarin ik zelf daarop invloed heb
 - Hoe ik dat waardeer
 - Hoe anderen dat waarderen (ook letterlijk)



Risicofactor Mens bij Informatiebeveiliging

- Rol-, taakopvattingen en integriteit:
 - Hoe ik naast eventuele formele instructie vind, dat ik mijn rol “moet” spelen / mijn taak “moet” uitvoeren
 - Hoe ik integriteit definieer en de wijze waarop ik dat van toepassing vindt zijn op mijn eigen denken en handelen
 - Cognitieve dissonantie
 - Attributie
 - Solidariteit
 - In- of exclusie



Risicofactor Mens bij Informatiebeveiliging

- Verwachtingen\ ervaringen:
 - “Er gaat toch niets mis als ik me niet aan al die regels houd.”
 - “Ze hadden mij moeten betrekken bij de totstandkoming van dat protocol”
 - “Software-ontwikkelaars maken zelf onveilige software; al die patches!!!”
 - “Zelfs die stemcomputers garanderen mijn privacy niet.”
 - “Er staat toch geen sanctie op.”



Risicofactor Mens bij Informatiebeveiliging

- Persoonlijkheid:
 - In- of externe attributie
 - Autoriteitsgevoeligheid
 - Positief of negatief zelfbeeld
 - Behoeftte aan orde en controle
 - Behoeftte aan macht
 - Risicomijdend of niet
 - Verantwoordelijkheidsgevoel



Risicofactor Mens bij Informatiebeveiliging

- (Bedrijfs-)cultuur:
 - Hoe gaan we om met autoriteit?
 - Hoe gaan we om met regels?
 - Hoe gaan we om met belonen of straffen?
 - Hoe gaan we om met eigenzinnigheid?
 - Hoe gaan we om met groepsnormen?



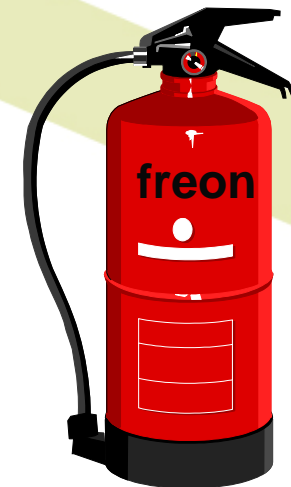
Risicofactor Mens bij Informatiebeveiliging

- Zijn voornoemde invloedsfactoren constant?
 - Zo ja, wat betekent dat voor IB?
 - Protocollen zijn oplossing
 - Gebruikersrechten en toegangscontrole zijn voldoende
 - Op medewerkers gerichte maatregelen
 - Zo nee, wat betekent dat voor IB?
 - Protocollen dekken niet alles af
 - Nood- of improvisatieprotocol nodig
 - Persoonlijkheid ook beschouwen
 - Aandacht voor cultuur en leiderschap
 - Foutenmarge acceptatie



Risicofactor Mens bij Informatiebeveiliging

- In elk geval:
 - Positie van en draagvlak voor IB'er
 - Risico's inventariseren (wie, wat, waar, wanneer)
 - Voorlichten (awareness) / Instrueren (ook klanten)
 - Audits uitvoeren
 - Juiste bedrijfscultuur "bewaken"
 - Noodplannen ontwerpen en testen





Dank voor uw
aandacht!

De Haagse Hogeschool
Academie voor ICT & Media Zoetermeer
079-3208787
S.E.Querido@hhs.nl
www.dehaagsehogeschool.nl

DE HAAGSE
HOGESCHOOL
ACADEMIE VOOR ICT & MEDIA
ZOETERMEER