



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.



Informatiebeveiliging

Onderwijs in waarden en normen!

Lectoraat Informatiebeveiliging Haagse Hogeschool

Cobie van der Hoek

Leo van Koppen

[Introductie]

- Lectoraat Informatiebeveiliging
 - Lector Dr. Marcel Spruit
 - Kenniskring met 5 docenten
- Activiteiten
 - Onderwijs (minor blok IB, module IB)
 - Onderzoek (honeypots, VPN, awareness)
- Invalshoeken
 - Technisch (netwerken)
 - Organisatorisch

[Competenties; ook bij IB]

- Kennis
 - Cryptografie, protocollen, firewalls, etc.
 - Beleid, bewustzijn, Plan, Do, Check, Act
- Vaardigheden
 - Uitvoeren van beveiligingsmaatregelen
 - Analyseren en adviseren inzake IB
- Attitude
 - Extra aandacht in de praktische situatie
 - ◆ Beoordeling
 - ◆ Werkvormen zoals in deze workshop

[Dilemma's]

- *Doel:* nadenken over IB-kwesties!
- Bevorderen van IB-bewustzijn
- Specifieke persoonlijke competenties m.b.t. informatiebeveiliging (zie Tinfon)
 - Waarborgen van:
 - ◆ vertrouwelijkheid
 - ◆ Integriteit

Niet alleen m.b.v. techniek, maar ook als mens

[Workshop]

- Werkwijze
 - Casus wordt voorgelegd
 - Aansluitend een dilemma
 - Reacties wordt gevraagd
 - Korte samenvatting, conclusie
 - Casus uitbreiden
 - Nieuw dilemma
 - Etc...

[Dilemma 1: gestolen toets]

Wat doe je?

- Je gaat uit op onderzoek en je wil de onderste steen boven hebben.

of

- Je gaat wel op onderzoek uit maar laat de cijfers de cijfers.

[Dilemma 2: regels opstellen]

Wat doe je ?

- Je besluit om in het eerstvolgende overleg met je collega's dit probleem te bespreken. Je komt met het voorstel dat er regels moeten worden opgesteld om dit soort situaties uit te sluiten.

of

- Je weet dat een strikte reglementering invoeren een heilloze zaak is, omdat het in de organisatie "cultuur" is (als een waarde wordt beschouwd) dat elke docent in dit soort zaken zijn eigen verantwoordelijkheid heeft.

[Dilemma 3: integriteit]

Wat doe je ?

- Je doet zelf niets maar wacht af totdat de Simon de systeembeheerder melding heeft gemaakt van de zaak !

of

- Je onderneemt actie en je gaat de zaak aankaarten, maar bij wie begin je ?
 - Simon de systeembeheerder
 - de directie
 - je gaat zelf de heren hackers aanspreken en ze ondervragen om ze vervolgens bij de directie te kunnen aanmelden als fraudeurs.

[Dilemma 4: privacy]

Wat doe je ?

- Je besluit om de vader de namen van mogelijke handlangers te geven.

of

- Je denkt, dit gaat me te ver en vindt dat de vader zonodig de politie maar moet inschakelen!

[Dilemma 5: schade?]

Wat doe je ?

- Je wijst het interview af en:
 - Besluit nu toch maar de directie in te schakelen uit angst voor je eigen positie.
 - hoopt dat het allemaal niet zo'n vaart zal lopen

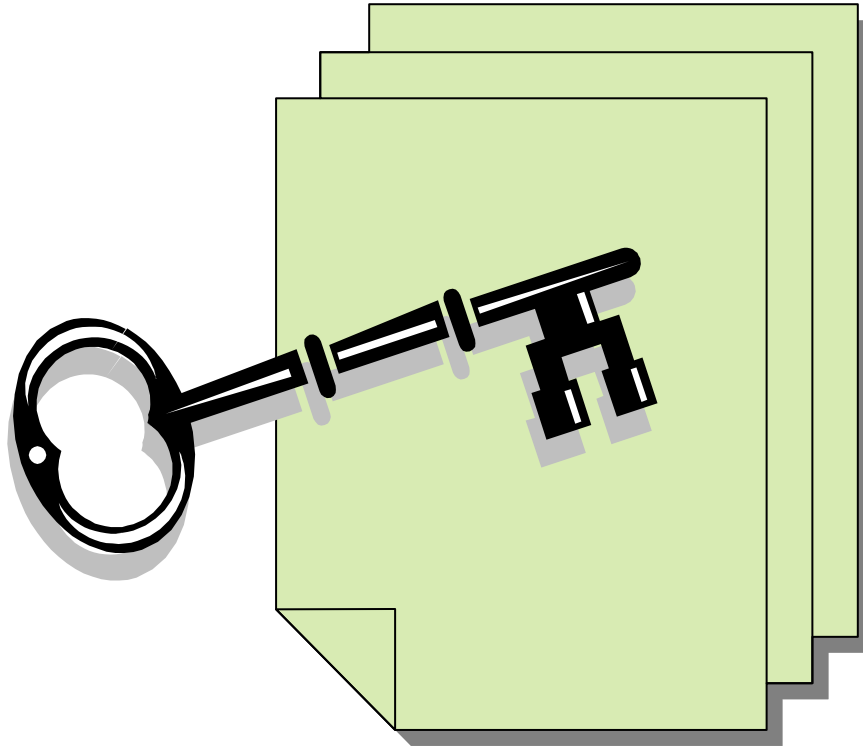
of

- Je stemt toe voor een interview:
 - nadat je de directie hebt geïnformeerd
 - maar spelt de journalist iets op de mouw en probeert op die manier
 - ◆ tijd te winnen
 - ◆ het brandje te blussen

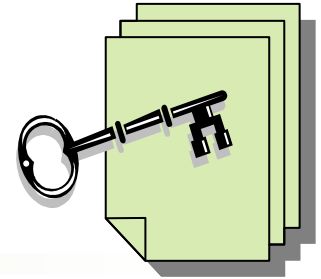
[Samenvatting; aspecten]

- 1^e ronde
 - Type maatregel, risicoafweging, integriteit
- 2^e ronde
 - IB-beleid, organisatorische maatregelen
- 3^e ronde
 - Integriteit (persoon, systeem)
- 4^e ronde
 - Privacy
- 5^e ronde
 - Imagoschade

[Minor Informatiebeveiliging]

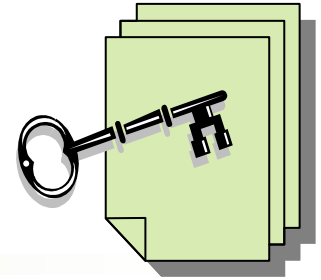


[Kenmerken minor IB

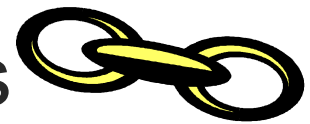
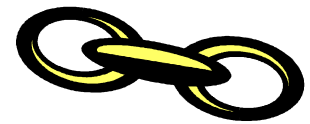


- Omvang 15 ECTS
- Aantrekkelijk (state of the art)
- Schaalbaar (I, BI, TI)
- Flexibel (fase in opleiding van student)
- Praktijkrelevantie
 - Externe certificering (GIAC + Security+)
 - Bedrijfsprojecten (quick scan, audits, etc)

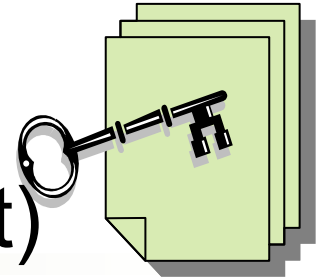
[Ontwerp



- Illustraties opstellen van IB'er
 - Volgens het nieuwe model van HBO-I
 - 3 nieuwe illustraties toegevoegd
 - ◆ IB-functionaris, IB-auditor, IB-specialist
- Competenties afleiden voor IB'ers
- Onderdelen minor IB:
 - Verplichte onderdelen → basis IB-kennis
 - Keuze → verdieping in lijn met major

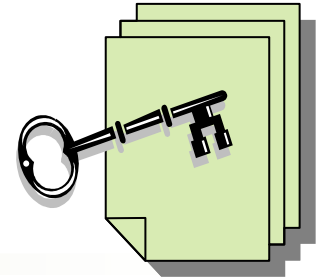


[Onderdelen Minor-IB (verplicht)



- Informatiebeveiliging (inleiding)
- Bedreigingen; hackingtechnieken
- Maatregelen; beveiligingsconcepten
- Cryptologie (=cryptografie + crypto-analyse)
- Netwerkbeveiliging
- Toegangsbeveiliging (logisch + fysiek)
- Operationeel beheer (security management)
- Risico-analyse; kwetsbaarheid, afhankelijkheid
- Awareness; mens is de zwakste schakel

[Onderdelen Minor-IB (keuze)



- Middleware (+ OS, Databases)
- Software
- Bedrijfscontinuïteit
- Wetgeving
- Social engineering
- Falende mens

[Tijd (?) voor vragen!]



Dank voor uw:

- komst
- aandacht
- medewerking

[Meer Informatie]

- via Internet (binnenkort)

informatiebeveiliging.thrijswijk.nl

- per email

- Cobie van der hoek:

hoc@thrijswijk.nl

- Leo van Koppen:

l.c.m.vankoppen@hhs.nl

