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.

UNIVERSITY OF APPLIED SCIENCES UTRECHT

Security in Onderzoek

Wiebe Wiersema
Lector Architectuur Digitale Informatie Systemen

Roelant Ossewaarde
Hogeschooldocent

Even voorstellen

Wiebe Wiersema, Bijzonder Lector

- Pragmatisch bruggenbouwer
- 7 jaar lector, 1 dag/week
- Focus op Bachelor Onderwijs
- 25 jaar ervaring in ICT

Roelant Ossewaarde, Hogeschooldocent

- Docent sinds twee jaar aan de HU
- Focus op data-analyse en security

Wat doet het lectoraat ADIS

Doelstellingen

- Actief bijdragen aan het “verzwaren” van het Bachelor Curriculum
- Studenten toegepast onderzoek laten doen
- Samenwerken met bedrijven uit de regio Utrecht

Onderzoekslijnen

- Kwaliteit van architectuur
- Gebruik / Toegevoegde waarde van Architectuur

We werken veel samen met zorg lectoraten

Casussen – RAAK Projecten

- Project “Godiva”
  - Doel is om fysiotherapeut in staat te stellen te kijken naar de motorische ontwikkeling van kinderen
  - Beelddata bank waar ouders filmpjes uploaden van hun kinderen die bepaalde oefeningen in doen.
  - Fysiotherapeuten kunnen deze filmpjes bekijken

- Project “Fit for the Future”
  - Doel is om fysiotherapeuten ondersteuning te geven bij de behandeling van zeldzame aandoeningen en de gegevens aan onderzoekers aan te bieden om behandelplannen te verbeteren
  - Kennis bank en Centrale opslag van patientbehandel data, uitkomsten van testen etc
  - Fysiotherapeuten hebben toegang nodig tot de gegevens

- Echte Data!

Hoofdpijn dossier

- Wat kan er gebeuren bij diefstal of lekken gegegvens?
  - Beschadiging patiënten
  - Negatieve publiciteit
  - Strafrecht / Civiele procedure

- Willen we als Hogeschool dit soort gevoelige gegevens in huis hebben?
- Hoe gaan we hier nou goed mee om?
- Wanneer doen we het goed?

Casus: Godiva en FitForFuture

Verschillende stakeholders

- Studenten, docenten: onderwijs genieten
  - +- 15 studenten
  - Cursus: “advanced software engineering”
- Onderzoekers: werkend systeem
- HU-security: veilig systeem

Subtiele druk in de organisatie:

- Onderzoekers moeten een veilig systeem hebben voor onderzoek.
- HU-security moet dat faciliteren.
- HU-beheer kan dat niet faciliteren (zo’n systeem is er niet).
- Ieder alternatief (buiten HU) is erger.

Casus: Godiva en FitForFuture

Security volgens geldende normen:

- NEN-7510, NEN-7512, NEN-7513 (2011)
  - Eisen aan beleg van verantwoordelijkheden
    - Responsible, Accountable, Consulted, Informed
  - Eisen aan beheersmaatregelen
- PCI-DSS (credit card payments)
  - Formuleert requirements aan het ontwikkelproces.
  - Specifieker voor implementatie-details.
- Studenten kennen in ieder geval de NEN-eisen
- Verwerking door opstellen van risico-analyse voor beide systemen door studenten aan het begin van onderwijsblok

Casus: Godiva en FitForFuture

Een typisch themaproject ziet het er zo uit:

PCI-DSS requirements:	Studenten	Docenten	HU
Build secure network	Responsible, Accountable		
Build secure system	Responsible, Accountable		
Protect data	Responsible, Accountable		
Maintain vulnerability program	Responsible, Accountable		
Implement Strong Access Control	Responsible, Accountable		
Monitor / test network	Responsible, Accountable		
Maintain security policy	Responsible, Accountable		

Casus: Godiva en FitForFuture

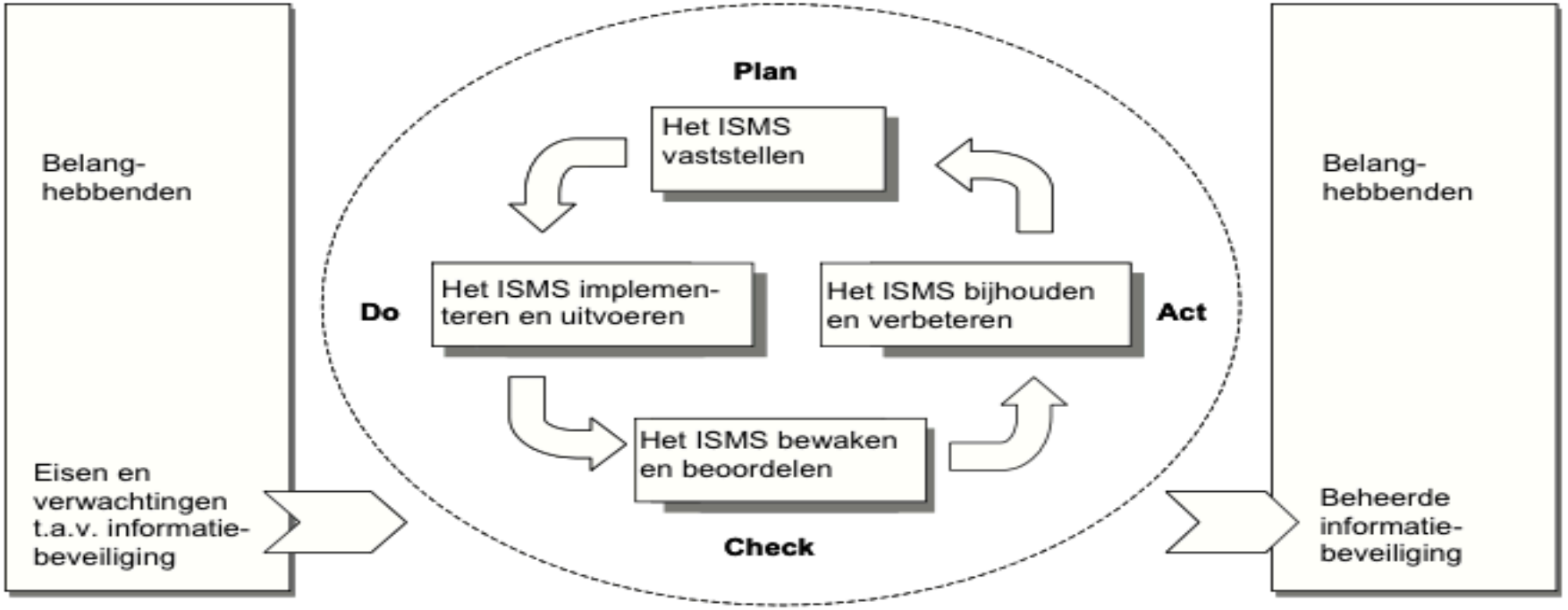
UNIVERSITY OF APPLIED SCIENCES UTRECHT

In een productieomgeving ziet het er zo uit:

	Studenten	Docenten	HU-security	HU-beheer
Build secure network			A	R
Build secure system	R		A	
Protect data	R		A	
Maintain vulnerability program		R	A	
Implement Strong Access Control	R		A	
Monitor / test network			A	R
Maintain security policy			R, A	R

Casus: Godiva en FitForFuture

Studenten stellen eigen security eisen op



- Eén team verantwoordelijk voor PLAN en CHECK
  - 3 studenten
- Drie teams verantwoordelijk voor DO en ACT
  - 10 studenten

Casus: Godiva en FitForFuture

Concrete organisatie van het PLAN/CHECK-team

- Heeft kennis van NEN-normen en PCI-standaard
- Implementeert test-strategie voor andere drie teams
- Heeft beslissende stem bij keuze voor technologie
  - Bv: “aspect-oriented architecture” vanwege logging en authenticatie

Externe partij aangewezen om eindproduct te testen:

- Security analysis
- Pentesting
- Review van documenten en procedures

Casus: Godiva en FitForFuture

Uitkomsten:

- Product voldoet aan de normen die HU stelt aan externe leveranciers
- HU-beheer vindt het leuk om mee te werken
- Cruciaal om organisatie mee te krijgen: rol van onderzoekers
- Juist security-eisen openen deuren in de organisatie.

Studentbeoordeling van Plan/Check-team:

- PCI-requirements net zo als functionele requirements
- Pass/No pass-oordeel van HU-security
- Kwaliteit van documentatie
- Adoptie bij mede-studenten

Discussie

- Wat kan er gebeuren bij diefstal of lekken gegevens?
  - Beschadiging patiënten
  - Negatieve publiciteit
  - Strafrecht / Civiele procedure
- Willen we als Hogeschool dit soort gevoelige gegevens in huis hebben?
  - Moeten we een leverancier zoeken?
  - Vertrouwen wij de cloud?
- Hoe gaan we hier nou goed mee om?
  - Hebben studenten voldoende besef?
- Wanneer doen we het goed?
  - CBP?
  - ISO 27K standaarden?
  - Security Architectuur

UNIVERSITY OF APPLIED SCIENCES UTRECHT

VRAGEN?