NORA werkdocument

Sessie 6

"In 3 klikken naar bouwstenen voor invulling van de eisen"

Katern Beveiliging

Bijgewerkt op 23 aug. 2013

Expertgroep NORA katern Beveiliging

Jaap van der Veen

Essentie Sessie 6

1. Opzet digitaal katern
   - Ambitie: “vanuit startpagina Beveiliging *in drie klikken* naar de bouwstenen voor de invulling van de eisen”
   - Bouwstenen met verbinding naar beveiligingdoelstellingen en de norm, in feite de middle out-middle in benadering. Vanuit eisen en doel-thema’s de naar bouwstenen, met normen en de verbinding naar boven: *Beleid* en naar beneden: *Beheersing/Control*
   - Startpagina: Doel_Functie_Gedrag_Structuur raamwerk
2. Scope
   - Beveiligingsbreed, we beginnen met Informatievoorzieningen
   - <Zie verder speakernotes>

De kracht van het katern zit in het vermogen om de gebruiker te kunnen ondersteunen en aansluiting te vinden op zijn informatiebehoefte door slimme beperking van het detailniveau

Voorbeeld BCM

Bedrijfscontinuïteit — Continuiteitsvoorzieningen Systeemintegriteit

Doelstellingen

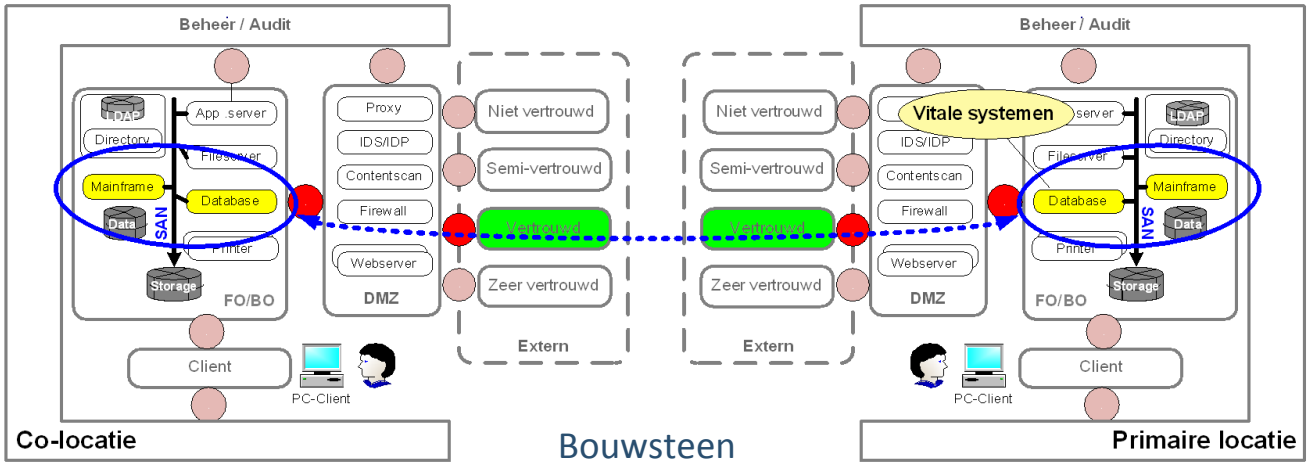
- De IT-voorzieningen voldoen aan het voor de diensten overeengekomen niveau van beschikbaarheid
- In de technische infrastructuur zijn functies werkzaam die de systeemintegriteit ondersteunen

Beheersmaatregelen

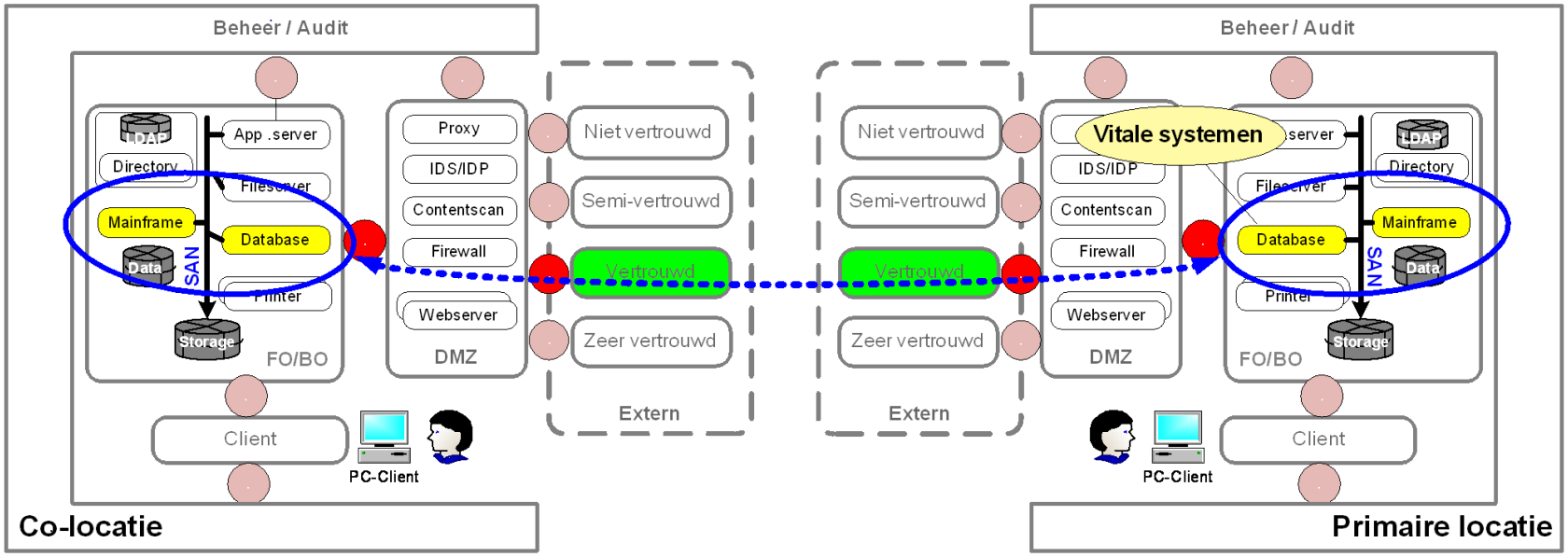
- Vanuit de Plannen Bedrijfscontinuïteit wordt bepaald in hoeverre delen van de technische infrastructuur dubbel worden uitgevoerd om single-points-of-failure te vermijden
- Verwerkingen zijn herstelbaar
- IT-voorzieningen proberen dreigende discontinuïteit van die voorzieningen te voorspellen dan wel te signaleren in een zo vroeg mogelijk stadium dat zij optreden

Referentie normen

BS 7.5.2
BS 7.5.3
HBB 16.2.1



Voorbeeld BCM



Implementatie richtlijnen

Dubbele uitvoering en spreiding van IT-voorzieningen

- Bij het vermijden van single points-of-failure kunnen de volgende maatregelen worden getroffen:

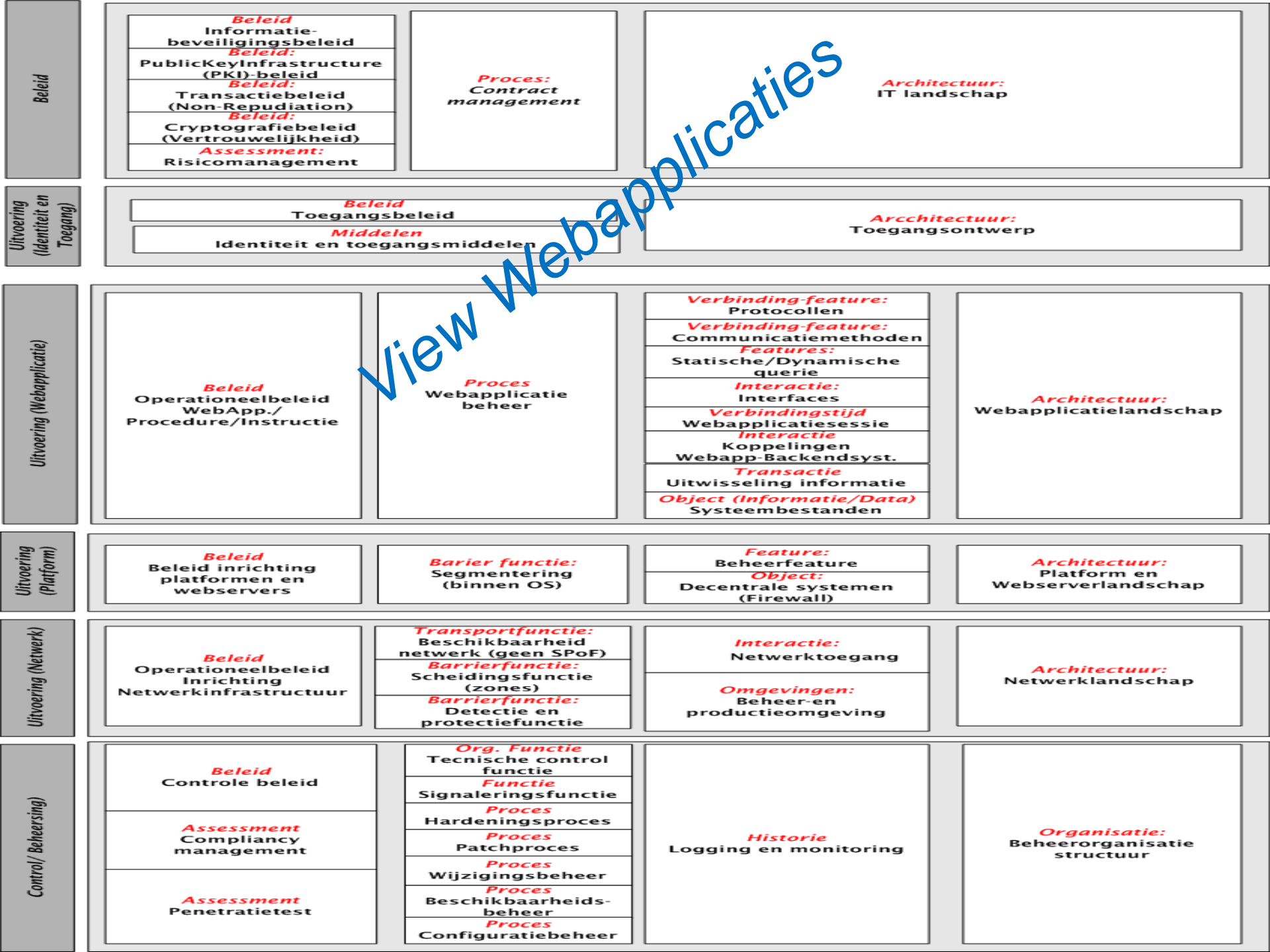
A) dubbele uitvoering van voorzieningen
B) zodanige plaatsing dat dubbele voorzieningen niet op één fysieke locatie zijn gesitueerd
C) geografische spreiding en op dezelfde technologie baseren
D) snelle beschikbaarheid van reserve-voorzieningen
E) uitwijkcontracten

"Startpagina in wording"

	Doelen	Functies	Gedrag	Structuur
Algemeen beleid	Bedrijfscontinuïteit	Continuiteitsvoorzieningen Systeemintegriteit	Normen/richtlijnen	Enterprise Architectuur
Specifiek beleid			Eisen	
Uitvoering	Gecontroleerde gegevensverwerking Geautoriseerde toegang van personen en systemen Borging vertrouwelijkheid en integriteit van gegevens Gecontroleerde gegevenstransport	Geprogrammeerde controles Identificatie, Authenticatie, Autorisiatie Onweerlegbaarheid berichtuitwisseling Zonering Filtering	Actoren Objecten	Beschouwings modellen Patronen
Specifiek beheersing	Beheersing aantoonbaar	Logging, Controle, Alarmering Rapportering	Procedures	Beveiligingsbeheer
Algemeen beheersing			Normen/richtlijnen	Governance model

Inhoud bereikbaar vanuit startpagina

Doel model	Functie Model	Gedrag model	Structuur model
Missie/Visie en Doelen Wet, Beleid, Strategie Stakeholders Risicomanagement Middelen	Org. Functies Systeem functies Processen Taken Taak Vereisten Managementtaken Primaire Taken Ondersteunende Taken	Resources Actoren Interacties Objecten Activiteiten Eigenschappen Toestanden Omgeving Historie Functionele vereisten Non Functionele vereisten	Enterprise Structure Business Structuur IT org. structuur Personeelstructuur Communicatie & Overlegstructuur Business Architecture IT Architecure Applicatie Architectuur Processing Architectuur Communicatie Architectuur


Beleid
Beleid
Informatie-beveiligingsbeleid
Beleid:
PublicKeyInfrastructure (PKI)-beleid
Beleid:
Transactiebeleid (Non-Repudiation)
Beleid:
Cryptografiebeleid (Vertrouwelijkheid)
Assessment:
Risicomanagement
Proces:
Contract management
Architectuur:
IT landschap
Uitvoering (Identiteit en Toegang)
Beleid
Toegangsbeleid
Middelen
Identiteit en toegangsmiddelen
Arcchitectuur:
Toegangsontwerp
Uitvoering (Webapplicatie)
Beleid
Operationeelbeleid WebApp./ Procedure/Instructie
Proces
Webapplicatie beheer
Verbinding-feature:
Protocollen
Verbinding-feature:
Communicatiemethoden
Features:
Statische/Dynamische querie
Interactie:
Interfaces
Verbindingstijd
Webapplicatiesessie
Interactie
Koppelingen Webapp-Backendsyst.
Transactie
Uitwisseling informatie
Object (Informatie/Data)
Systeembestanden
Architectuur:
Webapplicatielandschap
Uitvoering (Platform)
Beleid
Beleid inrichting platformen en webservers
Barier functie:
Segmentering (binnen OS)
Feature:
Beheerfeature
Object:
Decentrale systemen (Firewall)
Architectuur:
Platform en Webserverlandschap
Uitvoering (Netwerk)
Beleid
Operationeelbeleid Inrichting Netwerkinfrastructuur
Transportfunctie:
Beschikbaarheid netwerk (geen SPoF)
Barrierfunctie:
Scheidingsfunctie (zones)
Barrierfunctie:
Detectie en protectiefunctie
Interactie:
Netwerktoegang
Omgevingen:
Beheer-en productieomgeving
Architectuur:
Netwerklandschap
Control/ Beheersing)
Beleid
Controle beleid
Assessment
Compliancy management
Assessment
Penetratietest
Org. Functie
Tecnische control functie
Functie
Signaleringsfunctie
Proces
Hardeningsproces
Proces
Patchproces
Proces
Wijzigingsbeheer
Proces
Beschikbaarheids-beheer
Proces
Configuratiebeheer
Historie
Logging en monitoring
Organisatie:
Beheerorganisatie structuur
View Webapplicaties

View op IT-voorzieningen

Expertgroep NORA

Beschikbaarheid **I**ntegriteit **V**ertrouwelijkheid **C**ontroleerbaarheid

Eisen

Bedrijfscontinuïteit	Gecontroleerde gegevensverwerking	Borging vertrouwelijkheid en integriteit van gegevens	Gecontroleerde doorgang van gegevens	Logische toegang van personen en systemen	Beheersing aantoonbaar
Thema's					
Continuiteitsvoorzieningen Systeemintegriteit	Geprogrammeerde controles	Zonering, filtering, onweerlegbaarheid berichtuitwisseling		Identificatie, Authenticatie, Autorisatie	Logging, Controle, Alarmering Rapportering
Functies					
Doelstellingen	Doelstellingen	Doelstellingen	Doelstellingen	Doelstellingen	Doelstellingen
Doelen					
Beheersmaatregelen	Beheersmaatregelen	Beheersmaatregelen	Beheersmaatregelen	Beheersmaatregelen	Beheersmaatregelen
Maatregelen					
BCM	NCSC Web patronen	Thema patroon Encryptie	Thema patroon Koppelvlakken	Thema patroon IAM	Logging
Backup & Restore	NCSC Web patronen	Symmetrische Encryptie	Externe koppelvlakken	Identity Management	Security Information Event Management (SIEM)
Disaster Recovery	NCSC Web patronen	Public Key Infrastructure	Interne koppelvlakken voor de producieomgeving	Access Management	Logging STG Confi
Uitbesteding IT-diensten	NCSC Web patronen	Elektronische Handtekening	Interne koppelvlakken voor de ontwikkelomgeving	Federated IAM	
		Secure Email	Interne koppelvlakken voor beheer en audit	Single Sign On	
		Encryptie STG Confi	Koppelnetwerken met vertrouwde organisaties	Portaal - Toegangsserver	
		Sleutelhuis	Koppelvlakken STG Confi	Vertrouwd Toegangspad	
Bouwstenen					
Implementatierichtlijnen	Implementatierichtlijnen	Implementatierichtlijnen incl VIR-BI	Implementatierichtlijnen incl VIR-BI	Implementatierichtlijnen	Implementatierichtlijnen incl VIR-BI
Implementatie richtlijnen					

Zoneringsmodel, Client, Server, Netwerk, Virtualisatie

Beschouwings modellen

Uitvoering

1. Katern => normenkader onafhankelijk
   - Organisaties kunnen hun eigen kaders blijven gebruiken
   - Cross-referentie naar formele kaders ISO/BS/BIR/BIG/NCSC
   - NORA is geen nieuw normenkader maar een *toepassingskader* dat overzicht en inzicht geeft in beveiliging en refereert naar geaccepteerde normenkaders
2. Elektronisch navigeren door informatie
   - Dataset in Wiki of andere vorm, (APP, web- file of data-based) beschikbaar
3. Bronnen
   - Eigen beproefde kaders, Patronen PvIB, BIR-OB, whitepapers NCSC, NBV, industrie etc.

Actiepunten & trekkers

1. Scope infosyst.: verzamelen normen/richtl./patronen/practices (allen)
2. Aanpak: lifecycle breed: schrijven (Jaap)
3. Wiki: Ruimte voor katern in opbouw: (Eric/NORA beheerteam)
4. Beproefde teksten: toetsen in eigen org. (allen, vanuit best. kaders)
5. Modulair beschrijven, naar Wiki model (Jaap+ NORA beheer)
6. Prioriteit publicatie PvIB patronen (Jaap+ NORA beheer)
7. 10 geboden voor beveiliging (allen)
8. Beproeving content katern in eigen organisatie (allen, doorlopend)