centrum informatiebeveiliging
en privacybescherming

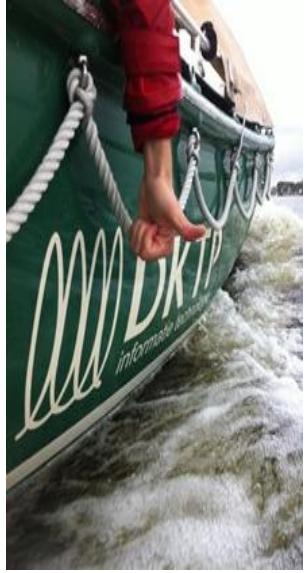
Grip op Secure Software Development

de rol van de tester

Rob van der Veer / Arjan Janssen

Testnet 14 oktober 2015

Even voorstellen..



Arjan Janssen
Directeur P&O
DKTP
a.janssen@dktp.nl

DKTP
informatie technologie

- DKTP is gespecialiseerd in het testen van software, bouwen van software en beheert omgevingen
- DKTP heeft meegewerkt aan de totstandkoming van Grip op SSD om kennis te delen en op te doen

Even voorstellen..

Rob van der Veer

Principal consultant security
Software Improvement Group
r.vanderveer@sig.eu

Software Improvement Group

- SIG toetst softwarekwaliteit en adviseert zowel opdrachtgevers als softwarebouwers
- SIG is kennispartner van het CIP
- SIG heeft veel ervaring met het sturen op softwarekwaliteit en heeft daarom meegewerkt aan de totstandkoming van Grip op SSD

Doel van de presentatie

- Kennis opdoen over de methode Grip op SSD
  - Uitleg over de methode Grip op SSD
  - Hoe Grip op SSD toe te passen

Laatste nieuws!

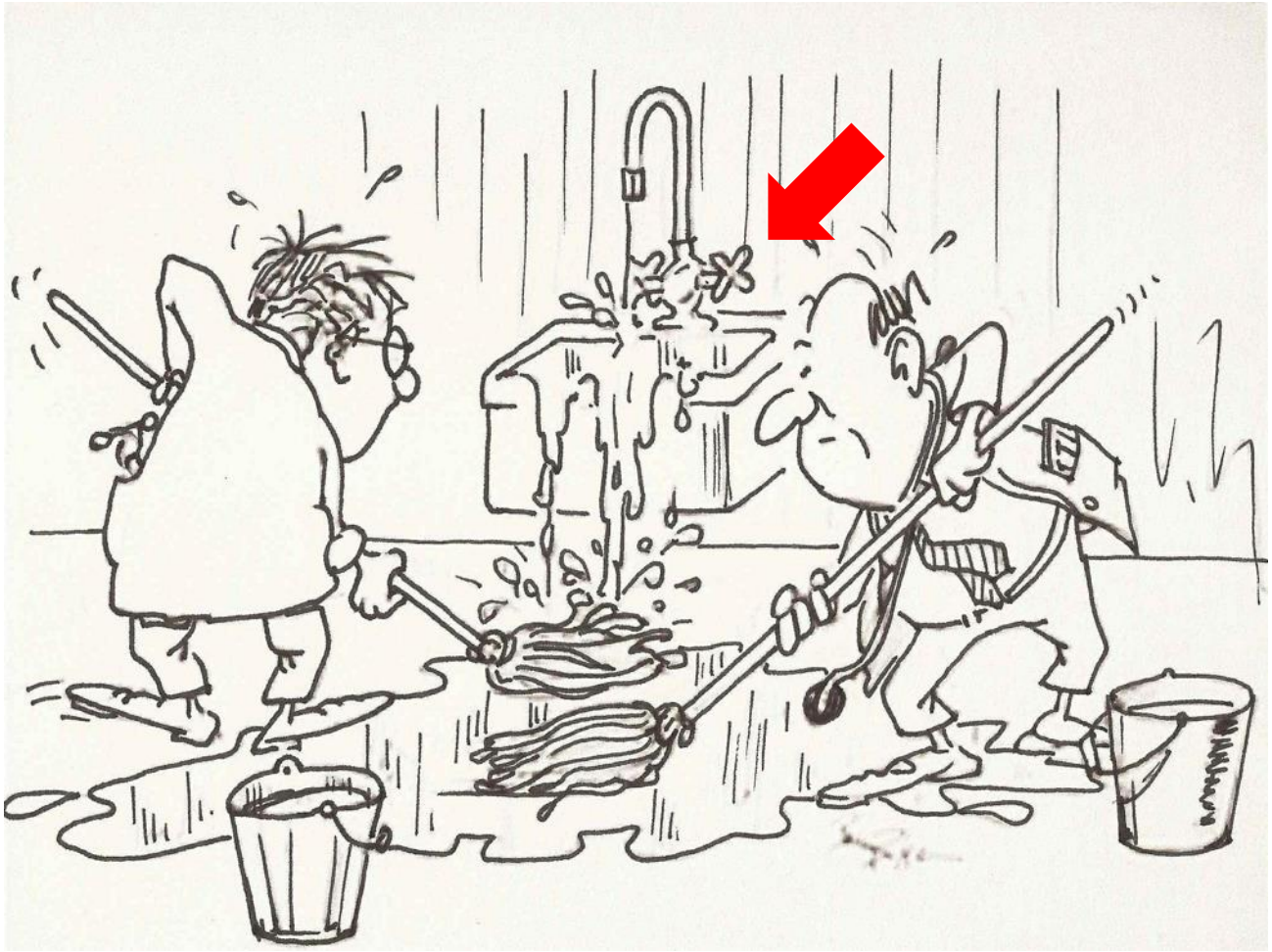
Meer cyberspionage in Nederland door buitenlandse overheden

Gepubliceerd: 14 oktober 2015 06:03
Laatste update: 14 oktober 2015 08:51

Nederland is het afgelopen jaar vaker doelwit geworden van digitale aanvallen vanuit andere landen. In het merendeel van de gevallen betreft het economische spionage door buitenlandse inlichtingendiensten.

Wat is het probleem?

Een groot deel van de security-incidenten komt door fouten tijdens software-ontwikkeling



“Wij gaan ervan uit dat een leverancier weet hoe je veilige software maakt”

“Ik dacht dat de hostingpartij dat zou regelen”

“Voor de beveiligingseisen, zie de OWASP website” of “De communicatie moet beveiligd zijn”

“We hadden eerlijk gezegd niet verwacht dat die security-eisen getoetst zouden worden”

“Die eisen sloegen totaal niet op wat we moesten maken – moest ik die echt serieus nemen?””

“O, leidt dat tot reputatieschade?”

“We versleutelen communicatie niet omdat dat niet hoeft, want het is te langzaam.”

“We doen al een penetratietest, dus”

Twijfelachtige reputatie

Tele2 schakelt klantenomgeving uit na datalek

Gepubliceerd: 18 februari 2015 10:37
Laatste update: 18 februari 2015 11:14

Tele2 heeft tijdelijk een gedeelte van zijn Mijn Tele2-klantenomgeving uitgeschakeld nadat meerdere klanten melding maakten van een datalek.

Minimaal zes klanten kregen afgelopen maandag de persoons- en bankgegevens van iemand anders te zien toen zij via de webversie van Mijn Tele2 probeerden in te loggen.

Dit bevestigde een woordvoerder van Tele2 tegenover NU.nl. Het datalek werd onder meer aan Tele2 gemeld via het forum van de telecomprovider.

In reactie op deze meldingen heeft Tele2 besloten de webversie van Mijn Tele2 voorlopig uit te schakelen voor klanten met een mobiel abonnement bij de provider.

Ook is het activeren van nieuwe Mijn Tele2-accounts tijdelijk niet meer mogelijk en kunnen bestaande wachtwoorden momenteel uit voorzorg niet worden gewijzigd.

Of het probleem zich breder heeft voorgedaan dan enkel bij de zes klanten die hiervan melding van hebben gemaakt, kon Tele2 nog niet zeggen. De provider onderzoekt de situatie momenteel.

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

HOME • DOE MEE • ONS WERK • OVER ONS • CONTACT • PERS BLOG

Afbeelding gebaseerd op Old log book van Adam Edmond (licentie: CC BY 2.0)

8 oktober 2012 14:01
Door Rejo Zenger

Zwartboek Datalekken

DATALEK: ZIEKENHUIS LEKT GEGEVENS 500.000 PATIËNTEN

Bits of Freedom heeft haar Zwartboek Datalekken weer uitgebreid. Een computersysteem met de gegevens van bijna 500.000 patiënten van een ziekenhuis bleek onvoldoende beveiligd.

Het computersysteem bevatte de medische dossiers van enkele tientallen patiënten. Ook het volledige patiëntenbestand van het ziekenhuis, bijna 500.000 patiënten, was in te zien. Daarin staan naast patiëntennummer, naam, adres, geboortedatum, telefoonnummer en burgerservicenummer ook gegevens over de partner. In een ander bestand staat welke patiënt op welke afdeling bekend is. Tussen de gegevens waren bovendien brieven tussen artsen, röntgenfoto's, echo's, hartfilmpjes, medicatielijsten, recepten, diagnoses, diverse soorten scans, behandelplannen en laboratoriumuitslagen te vinden.

De computer stond in een datacenter van een provider en lijkt al lange tijd onvoldoende beveiligd te zijn. Het lijkt er ook op dat de gegevens via een onversleutelde verbinding op de server werden gezet en het wachtwoord van de beheerder erg gemakkelijk te raden was. De computer werd gebruikt voor het digitaliseren van papieren dossiers.

Wat doen we aan het probleem?

Centrum voor Informatiebeveiliging en Privacybescherming (CIP)

expertisecentrum voor informatiebeveiliging en privacybescherming
van, voor en door overheidsorganisaties.
deskundige marktorganisaties als kennispartners deelnemen.

Bron: www.cip-overheid.nl

Partners en kennispartners

Grip op SSD producten
(www.gripopssd.org)

- Methode handboek
- SIVA beveiligingseisen
- Trainingsmateriaal testers
- Ervaringsdocumentatie
- Beveiligingsovereenkomst
- Werk in uitvoering:
  - Mobile requirements
  - Test tooling & proces

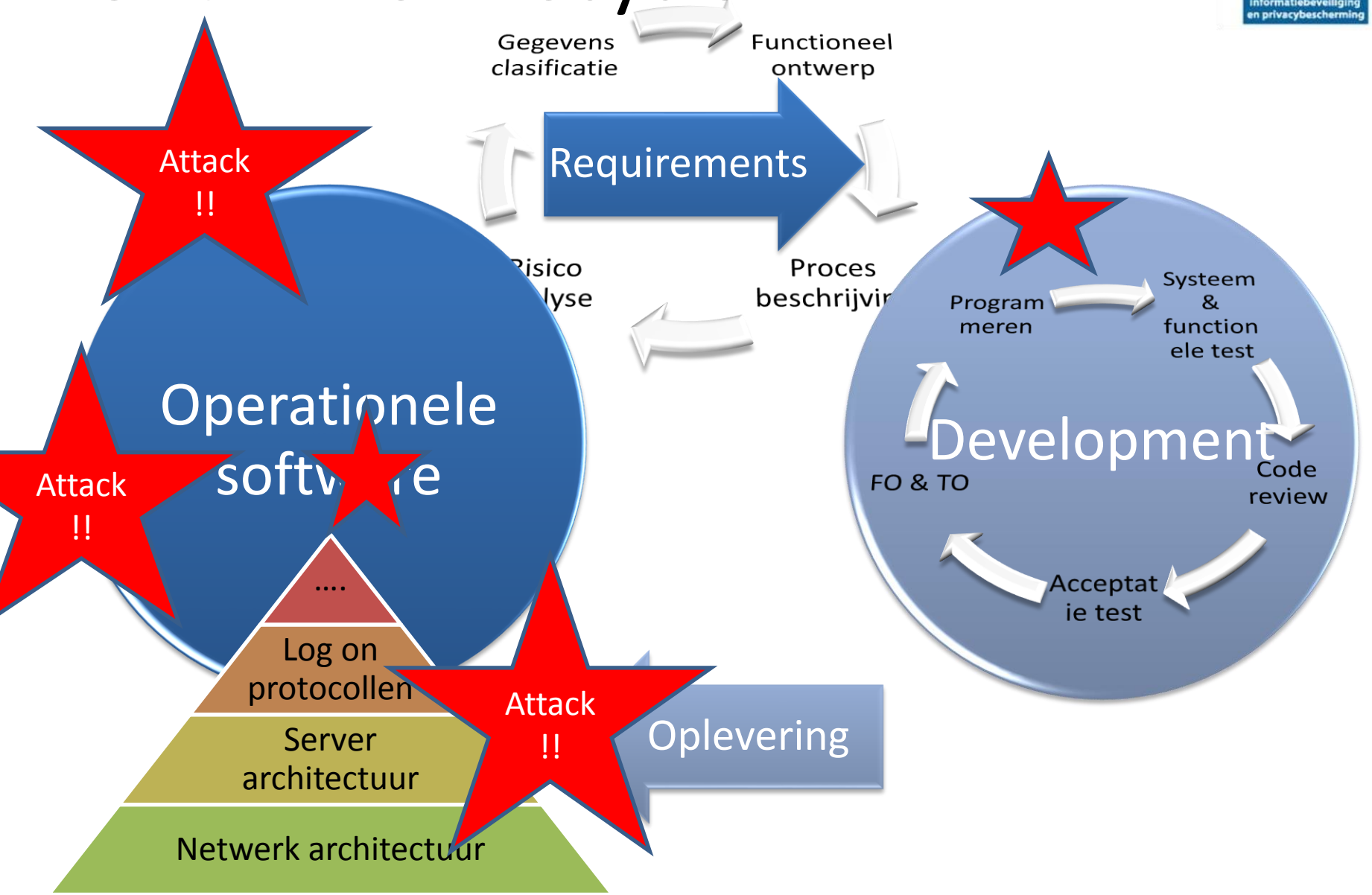
Oorzaken onveilige software

- Beveiligingseisen zijn afwezig of onduidelijk en niet op maat
- Er wordt niet of laat getoetst, hierdoor ‘schiet security er bij in’
- Opdrachtgever heeft te weinig risico-overzicht
- Bestaande standaarden bieden te weinig houvast
- Kennisniveau softwarebouwers schiet soms tekort
- Er wordt te weinig hergebruikt wat zich al bewezen heeft

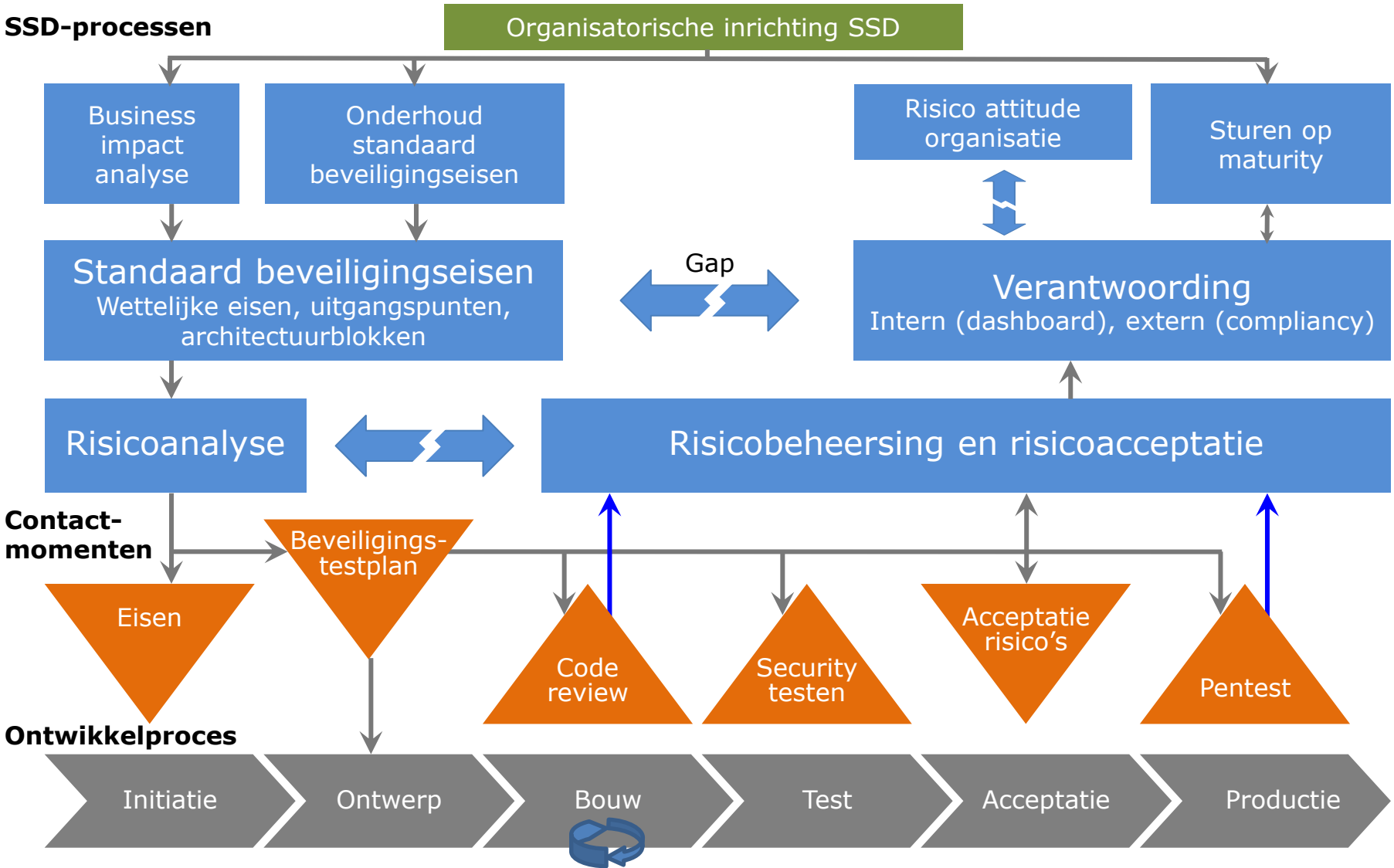
Hoe toets je security?

- En wat is daarvoor nodig?
- Wat doet een tester aan security testen?
- Wie is er verantwoordelijk voor security?

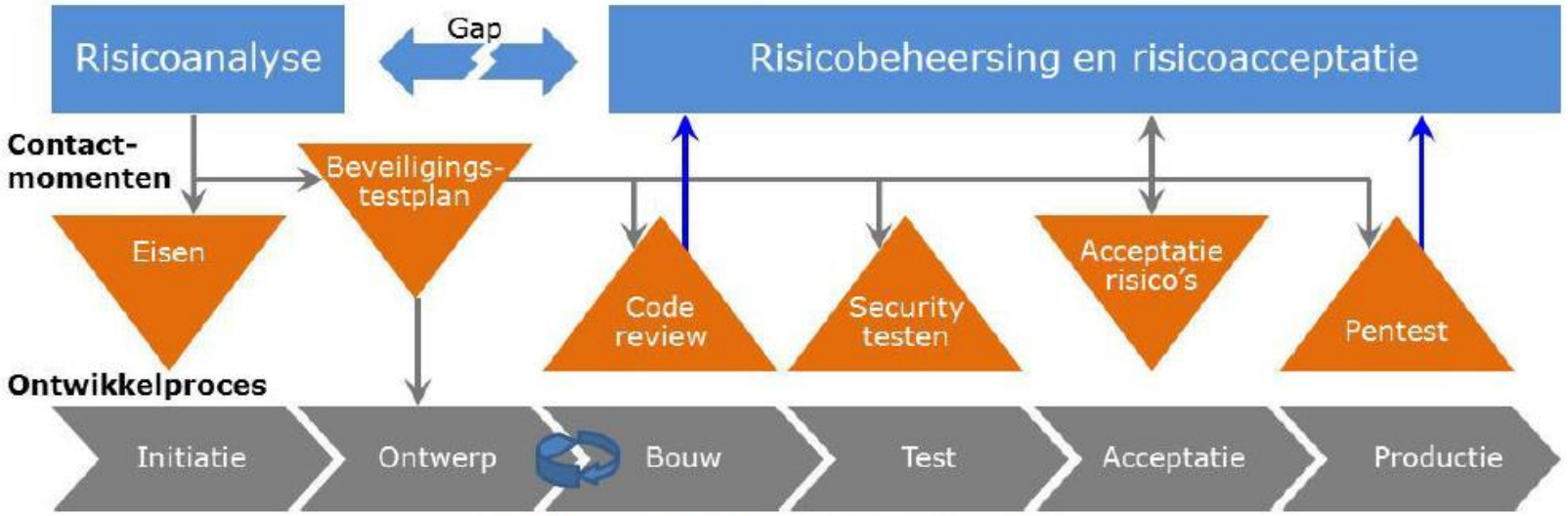
Ontwikkel lifecycle



Kom in contact en in control



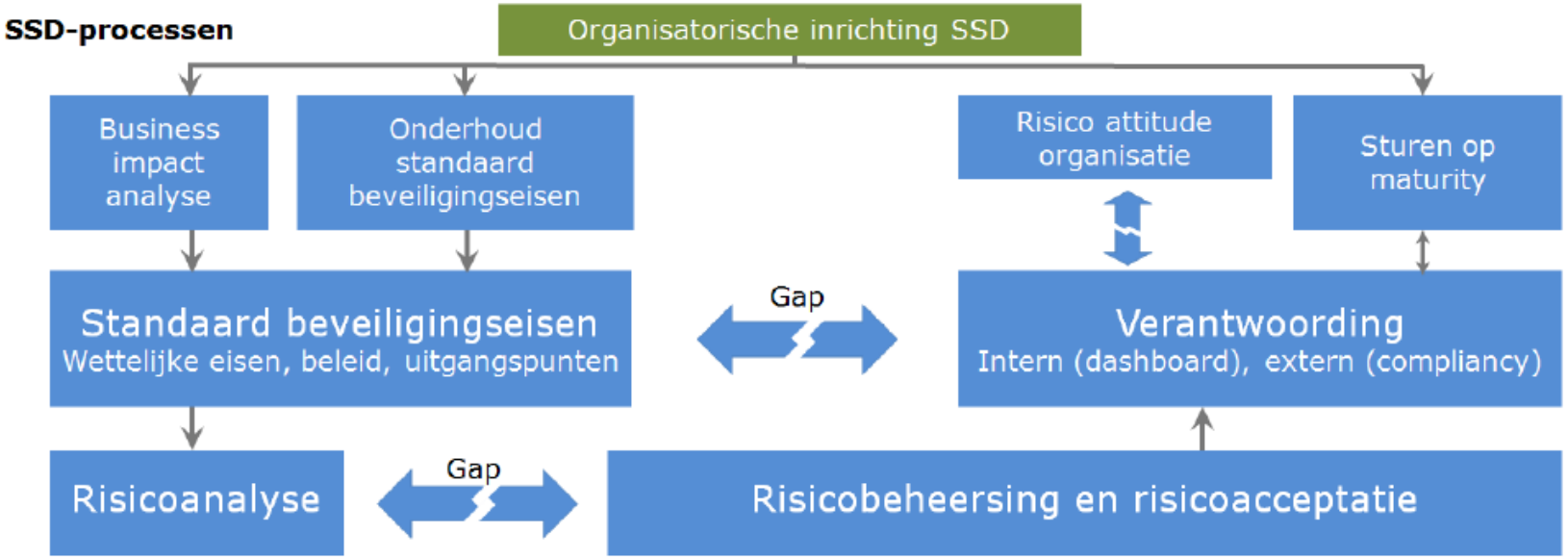
pijler 1: Contactmomenten



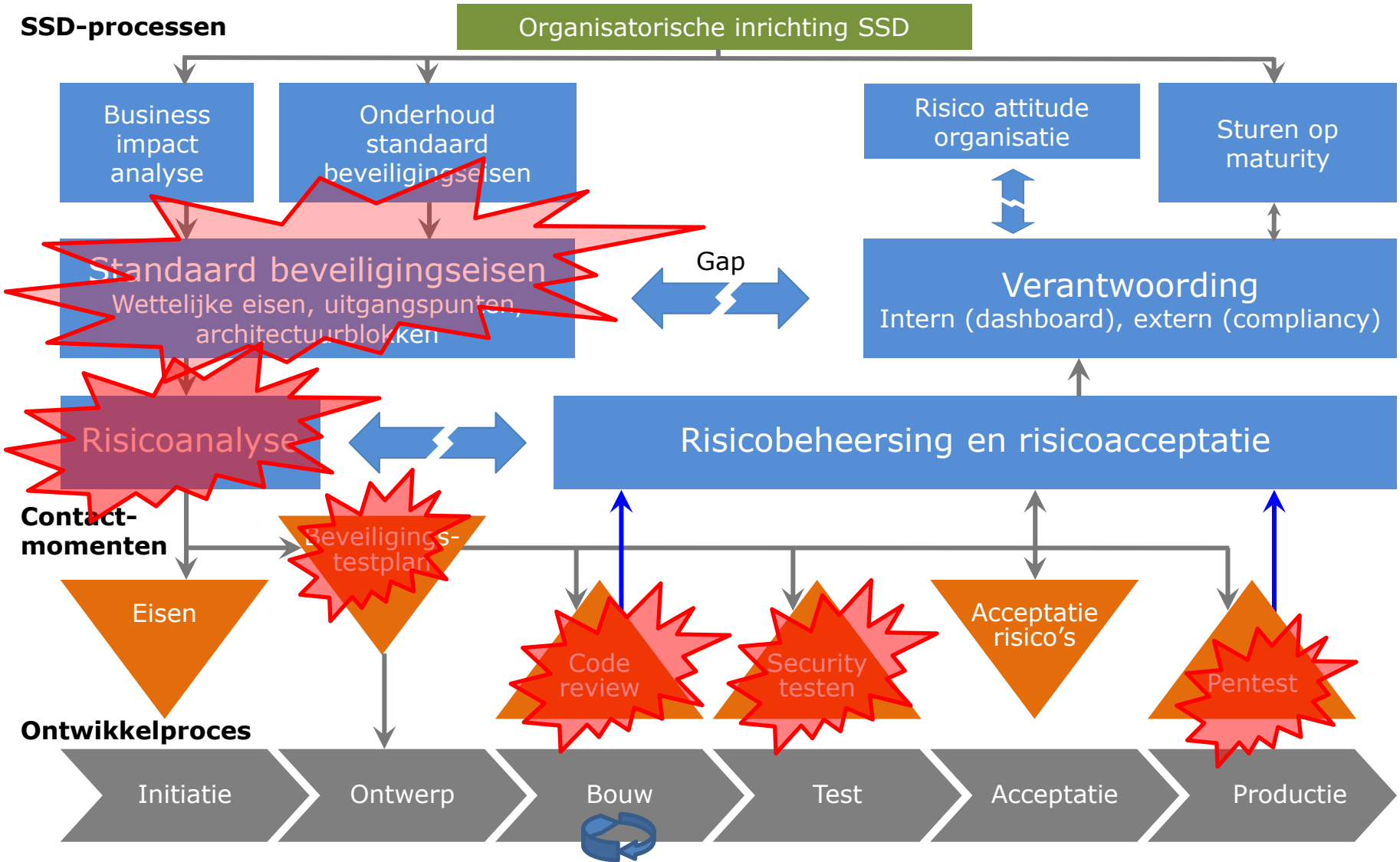
Figuur 3: pijler 1 - Contactmomenten

pijler 2: standaard beveiligingseisen

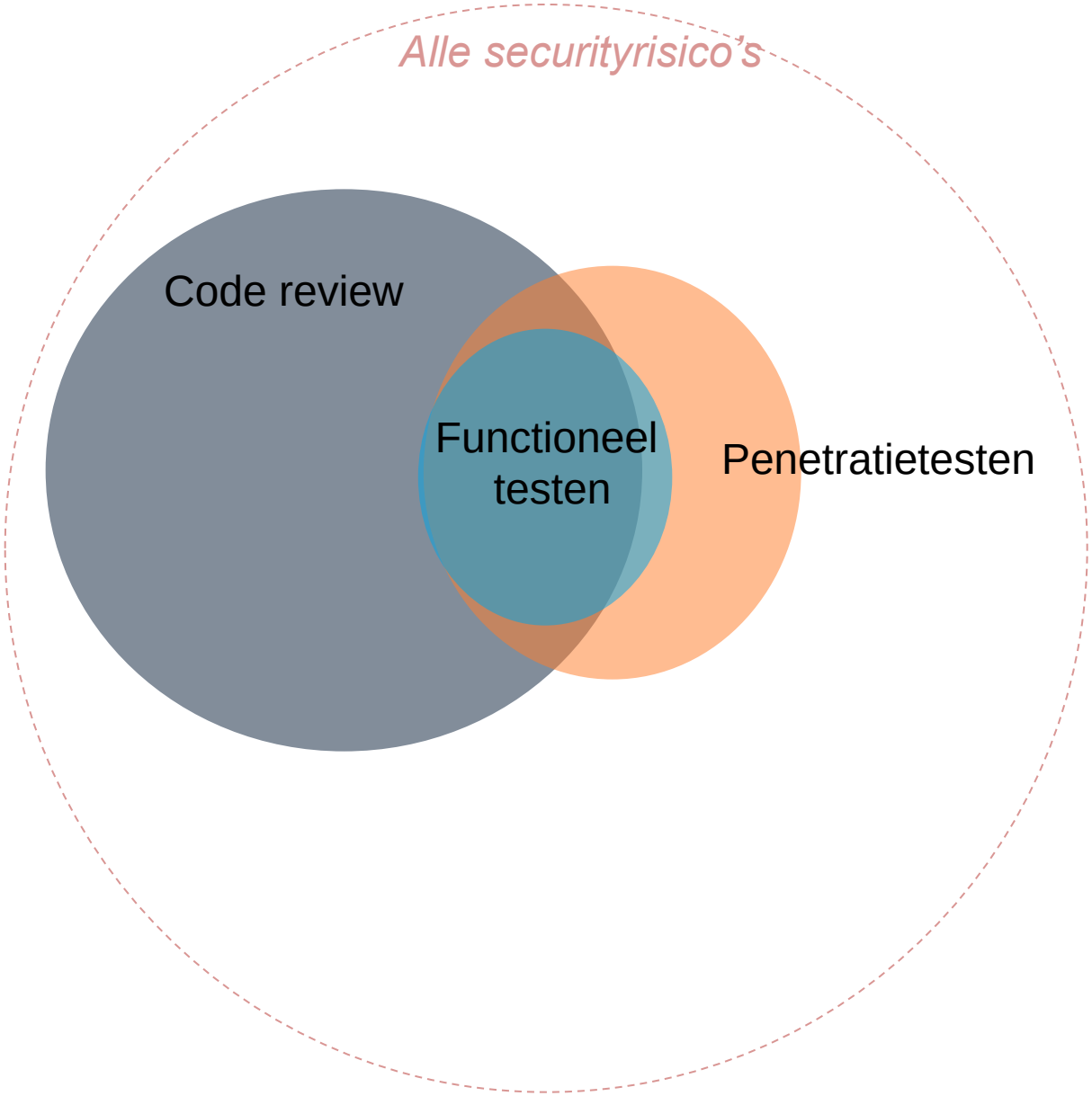
pijler 3: SSD-processen



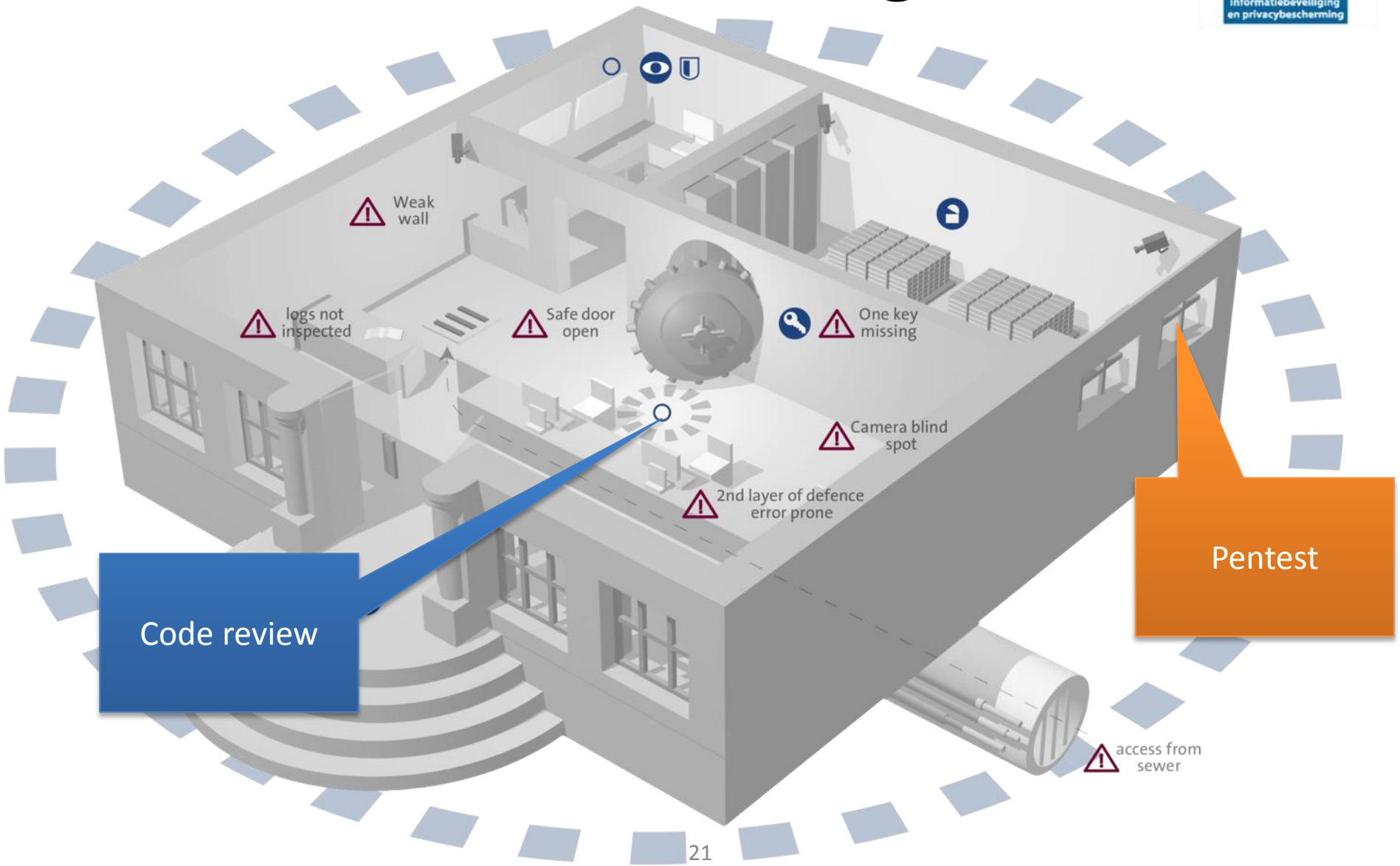
Kom in contact en in control



Toetsmethodes



Toetsmethodes - analogie



Toetsmethodes vergeleken

Code review	Functioneel testen	Penetratietesten
Toets of security is ingebouwd in ontwerp en broncode	Toets correcte werking	Toets non-functioneel
Kan in vroege fase	Werkend product	Werkend product
Fortify, Findbugs, Appscan, Checkmarx	Selenium, Ranorex, Test complete	BurpSuite, Zed Attack proxy, Lapse+
Vind 78% kwetsbaarheden*		Vind 43% kwetsbaarheden
Kijkt in alle lagen	Beprekt zich tot gespecificeerde functies	Beperkt zich tot lagen waartoe toegang is
Kosten €€€€	Kosten €	Kosten €€€

* Bron: Matthew Finifter, David Wagner. Exploring the Relationship Between Web Application Development Tools and Security. WebApps 2011

Voorbeeld eis SSD-14

SSD-14 Borgen van Sessie Authenticiteit					
Criterium (wie en wat)	De (web)applicatie hanteert bij de sessienummering op een onvoorspelbare wijze van nummeren en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.				
Doelstelling (waarom)	Het voorkomen van misbruik van een nog openstaande sessie, die door de oorspronkelijke gebruiker niet meer wordt gebruikt.				
Risico	Als een andere persoon een nog openstaande sessie kan oppakken, geeft dit de mogelijkheid van misbruik van de identiteit van de oorspronkelijke gebruiker.				
Referentie	NCSC	NIST	ISO27002		
	B4-2	SC-23			

/01	onvoorspelbare wijze van nummeren
/01.01	Een sessie-ID is voldoende sterk, namelijk een lang random nummer, om deze onvoorspelbaar te maken.
/01.02	De webapplicatie genereert steeds een nieuw random sessie-ID bij het inloggen en het opnieuw inloggen van een gebruiker.

/02	actief beëindigd
/02.01	De webapplicatie vernietigt aan de serverzijde actief de sessie bij het uitloggen van een gebruiker op de applicatie.

Functioneel testen SSD-14

SSD-14 Borgen van Sessie Authenticiteit					
Criterium (wie en wat)	De (web)applicatie hanteert bij de sessienummering op een onvoorspelbare wijze van nummeren en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.				
Doelstelling (waarom)	Het voorkomen van misbruik van een nog openstaande sessie, die door de oorspronkelijke gebruiker niet meer wordt gebruikt.				
Risico	Als een andere persoon een nog openstaande sessie kan oppakken, geeft dit de mogelijkheid van misbruik van de identiteit van de oorspronkelijke gebruiker.				
Referentie	NCSC	NIST	ISO27002		
	B4-2	SC-23			

- Kan een sessie worden hergebruikt na uitloggen?
  1. Log uit
  2. De applicatie mag niet meer werken
  3. Ga terug in browser: de applicatie mag niet meer werken

Penetratietest SSD-14

SSD-14 Borgen van Sessie Authenticiteit					
Criterium (wie en wat)	De (web)applicatie hanteert bij de sessienummering op een onvoorspelbare wijze van nummeren en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.				
Doelstelling (waarom)	Het voorkomen van misbruik van een nog openstaande sessie, die door de oorspronkelijke gebruiker niet meer wordt gebruikt.				
Risico	Als een andere persoon een nog openstaande sessie kan oppakken, geeft dit de mogelijkheid van misbruik van de identiteit van de oorspronkelijke gebruiker.				
Referentie	NCSC	NIST	ISO27002		
	B4-2	SC-23			

- Haal het sessienummer uit de cookie en analyseer of het patronen heeft en probeer een bestaande sessie te raden door scripts te schrijven
- Injecteer het sessienummer opnieuw in de cookie na uitloggen en probeer of diverse URL's werken
- Laat een tool willekeurige sessienummers raden en probeer zo een sessie te 'hijacken'

Code review SSD-14

SSD-14 Borgen van Sessie Authenticiteit					
Criterium (wie en wat)	De (web)applicatie hanteert bij de sessienummering op een onvoorspelbare wijze van nummeren en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.				
Doelstelling (waarom)	Het voorkomen van misbruik van een nog openstaande sessie, die door de oorspronkelijke gebruiker niet meer wordt gebruikt.				
Risico	Als een andere persoon een nog openstaande sessie kan oppakken, geeft dit de mogelijkheid van misbruik van de identiteit van de oorspronkelijke gebruiker.				
Referentie	NCSC	NIST	ISO27002		
	B4-2	SC-23			

- Behoort de gebruikte randomiseringsfunctie tot de lijst van erkende functies?
- Is het sessie-ID minimaal 128 bits?
- Zien we logica die de sessie-informatie daadwerkelijk verwijdert?

Code review

- 3 niveaus
  - Tooling bij ontwikkelaars
  - Peer review binnen ontwikkelorganisatie
  - Externe review

Penetratietesten

- 3 niveaus
  - Functioneel testen
  - Gebruik van tooling
  - Gebruik van ethical hacking vaardigheden

Starten met Grip op SSD

- Awareness
- Volwassenheid
- Standaard beveiligingseisen
- Business impact analyse

Acteren naar volwassenheid

Nog niet

		SSD-processen				
5		dezelfde prestatie-indicatoren leveranciers	dezelfde tooling en prestatie-indicatoren leveranciers	dezelfde tooling en prestatie-indicatoren leveranciers	pentest na meldi beveiligings	
4			e aanpak lerlinge	hogere voorspelbaarheid met kortcyclische	onderdeel acceptati	
3			rd v riti me		diek skr ster	
2			efsg		skr	
1		kopie baseline beveiligingseisen	op ad-hoc basis	op ad-hoc basis	slechts na beveiligingsincidenten	acceptatie zonder vervolgafspraken met applicatie-eigenaar
CMM-niveau		Beveiligingseisen	Code review	Testen en toetsen	Pentesten	Risicoacceptatie

Security by design

7. Meenemen context:
- BIA en IB risico-analyse
- Security architectuur

8. Rapp ges op de afwijkingen (Rood/Groen)

5. Feedback leveranciers:
- Eerst als bijlage op versie in de contracten.

4. Vergroten bewustzijn:
- Campagneleider
- Voorbeeld publiceren

6. Formele acceptatie gedoogsituatie

- Uitleg methode aan de IM's
- Contract leveranciers

- Uitleg van de methode
- Uitleg van de baseline

- Inventa satie hanteren baseline

Beveiligingseisen

3.15. SSD-14: Borgen van Sessie Authenticiteit

SSD-14 Borgen van Sessie Authenticiteit					
Criterium (wie en wat)	De (web)applicatie hanteert bij de sessienummering op een onvoorspelbare wijze van nummeren en bij het uitloggen van de gebruiker wordt de sessie actief beëindigd.				
Doelstelling (waarom)	Het voorkomen van misbruik van een nog openstaande sessie, die door de oorspronkelijke gebruiker niet meer wordt gebruikt.				
Risico	Als een andere persoon een nog openstaande sessie kan oppakken, geeft dit de mogelijkheid van misbruik van de identiteit van de oorspronkelijke gebruiker.				
Referentie	NCSC	NIST	ISO27002		
	B4-2	SC-23			

Toelichting

Een sessie (via http) tussen de (web)applicatie en de gebruiker krijgt een unieke sessie-ID. Na het uitloggen van de gebruiker dient de sessie actief te worden beëindigd door de webapplicatie om te voorkomen dat een andere persoon de nog openstaande sessie kan oppakken en hiermee verder kan werken.

In dit kader wordt ook aan het sessie-ID eisen gesteld, onder andere dat deze onvoorspelbaar is. Hiertoe wordt een nummer gebruikt met voldoende lengte en wordt een volgend sessie-ID random gekozen.

SSD Dashboard

ja	Voldoet aan de eis.
nee	Voldoet niet aan de eis.
nvt	De eis is voor de applicatie niet van toepassing
deels	Afspraken gemaakt met applicatie-eigenaar over de afwijking
	Nog geen constatering

Test Line	Applicatie complex	Datum laatste wijziging	SSD versie	Applicatie	SD-4B	SD-5	SD-6	SD-7	SD-8	SD-9	SD-10	SD-11	SD-12A	SD-12B	SD-13	SI 1
		28-jan-14	1.85			nvt	nvt	nvt		nvt	nvt	nvt	nvt	nvt	nvt	
		17-okt-13	1.85			nvt	ja	ja		nee	ja	ja	ja	ja	nee	
		27-mrt-14	1.85			nvt	ja	ja		nee	ja	nee	nee	nee	nee	
		4-nov-13	1.85			nvt	nee	ja		ja	ja	ja	ja	ja	ja	
		11-nov-13	1.85			nvt	nee	ja		nee	ja	nvt	nee	nee	nee	
		11-nov-13	1.85			nvt	ja	ja		ja	nee	nee	nee	nee	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	nee	ja		nvt	nvt	nvt	ja	ja	ja	
		4-nov-13	1.85			nvt	nee	ja		ja	ja	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	ja		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	
		4-nov-13	1.85			nvt	ja	nvt		ja	nee	ja	ja	ja	ja	

Succesvol testen met behulp van de methode ‘Grip op SSD'

Iedereen weet wat van hem of haar wordt verwacht.

- ✓ Begin met een minimum baseline.... en start met het dashboard.

Comply or explain

- ✓ Stel de beveiligingsrisicoanalyse verplicht v alle IV-projecten

PIA

WBP

- ✓ Baselines en risicoanalyses maken is een vak:
  - ✓ Organiseer kennis

CIP netwerk

- ✓ Zet de methode niet om in een groot implementatieplan

Wat levert SSD op?

- ✓ Veilige software
- ✓ Minder aanpassingen achteraf
- ✓ Minder incidenten
- ✓ Versterkt de betrouwbaarheid

Vragen?

Bedankt voor uw aandacht!

Rob van der Veer (SIG)
Arjan Janssen (DKTP)

www.gripopssd.org