Resultaten High Speed risicoanalyse Infoepd (1/2)

Front-end bedreigingen	Aspect			Reputatie Risico	Impact (hoe erg)	Kans (hoe waarschijnlijk)
	B	I	V			
Hacker onderschept webformulieren verzonden via Internet			X	Hoog	Hoog: persoonsgegevens komen in onbevoegde handen	Hoog:
Hacker onderschept UZI-formulieren via Internet			X	Hoog	Hoog+: naast persoonsgegevens komen ook bedrijfskritische gegevens in onbevoegde handen	Hoog:
Hacker manipuleert webformulieren verzonden via Internet		X	X	Hoog	Hoog: verwerking van persoonsgegevens inzichtelijk en te wijzigen door onbevoegden	Midden: met vlagen om publiciteit te zoeken maar uitvoering vergt meer kennis (zoals Cross Site Scripting)
Hacker manipuleert UZI-formulieren verzonden via Internet		X	X	Hoog	Hoog+: verwerking van persoonsgegevens en bedrijfs-kritische gegevens inzichtelijk en te wijzigen door onbevoegden	Midden: met vlagen om publiciteit te zoeken maar uitvoering vergt meer kennis over verwerking
Inhoud website veranderd door hackers met CMS toegang	X	X	X	Middel	Hoog: onbevoegde inzage en wijziging van persoonsgegevens en informatie op Infoepd mogelijk	Midden: een gerichte aanval nodig maar waarschijnlijk om publiciteit te zoeken
Inhoud website veranderd door hackers zonder CMS toegang	X	X		Middel	Midden: geen correcte informatie en functionaliteit beschikbaar	Hoog: relatief makkelijk uit te voeren om publiciteit te zoeken
Website onbeschikbaar door DOS-aanval hackers	X			Midden+	Laag: onbeschikbaarheid kan van korte duur zijn omdat situatie controleerbaar is	Hoog:
Hacker verkrijgt toegang tot persoonsgegevens opgeslagen in interne systemen		X	X	Hoog	Hoog+: grotere hoeveelheden persoonsgegevens inzichtelijk en te wijzigen door onbevoegden	Midden+: met vlagen om publiciteit te zoeken
Hacker manipuleert functionaliteit van interne systemen	X	X	X	Hoog	Hoog+: verwerking van gegevens inzichtelijk en te wijzigen door onbevoegden met mogelijke onbeschikbaarheid als gevolg	Midden: met vlagen om publiciteit te zoeken maar uitvoering vergt meer kennis

Resultaten High Speed risicoanalyse Infoepd (2/2)

Back-end bedreigingen	Aspect			Reputatie Risico	Impact (hoe erg)	Kans (hoe waarschijnlijk)
	B	I	V			
Inhoud website veranderd door fouten redacteuren	X	X		Midden	Laag: betreft kleine hoeveelheden informatie en tijdige detectie en reactie mogelijk	Hoog: fouten door aanpassingen via komen relatief vaak voor
Inhoud website veranderd door apparatuurstoring	X	X		Midden	Midden: kan grotere hoeveelheden informatie betreffen en opvolging vergt meer inspanning	Hoog: veel afhankelijkheden tussen onderlinge leveranciers
Functionaliteit systemen veranderd door apparatuurstoring	X	X	X	Midden	Midden+: geen gerichte aanval maar beschikbaarheid, integriteit en vertrouwelijkheid mogelijk in gevaar en impact mogelijk groter dan bij een beheerfout	Hoog: veel afhankelijkheden tussen onderlinge leveranciers
Functionaliteit systemen veranderd door beheerfouten	X	X	X	Midden	Midden: geen gerichte aanval maar beschikbaarheid, integriteit en vertrouwelijkheid mogelijk in gevaar	Middel: beheerfouten komen door dynamisch omgeving en wijzigende afspraken relatief veel voor
Website onbeschikbaar door apparatuurstoring	X			Midden+	Midden: sterk afhankelijk van reactiesnelheid betrokken leveranciers	Hoog: veel afhankelijkheden tussen onderlinge leveranciers
Website onbeschikbaar door beheerfouten	X			Midden+	Midden: duur onbeschikbaarheid sterk afhankelijk van oorzaak maar deze is eenvoudiger te traceren dan overmacht	Middel:
Website onbeschikbaar door overmacht	X			Midden	Midden+: duur onbeschikbaarheid moeilijk te beheersen door onvoorspelbare situaties	Midden: oals oververhitting, brand, waterschade, etc.
Geen gestructureerd Service Level Management	X	X	X	Laag	Hoog: onvoldoende afspraken voor beveiligingmaatregelen leiden tot inzage en wijziging van gegevens door onbevoegden en onbeschikbaarheid	Hoog+: dynamische technologische omgeving in aanbouw waarin veel ad hoc toevoegingen en wijzigingen plaatsvinden