Basisnormen Beveiliging en Beheer ICT-infrastructuur

Basisnormen Beveiliging en Beheer ICT-infrastructuur

PI/DO
Platform Informatiebeveiliging
B. Bokhorst
R. Kuiper
S. Mekking
P. Mercera
R. Torabkhani

Uitgeverij LEMMA BV – Utrecht – 2003

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden auteur(s), redactie en uitgever geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

ISBN 90-5931-228-7
NUR 980

http://www.lemma.nl
infodesk@lemma.nl

Omslagontwerp en typografie: Twin Design BV, Culemborg

Voorwoord

Het Platform Informatiebeveiliging (PI) heeft als doel 'het bevorderen van de beveiliging van alle belangen betreffende gegevensverwerking, -opslag en -transport, alles in de ruimste zin van het woord'. Binnen deze doelstelling wordt het ontwikkelen van aanvaardbare richtlijnen voor de praktische inrichting van informatiebeveiliging als essentieel onderwerp gezien. Door het gezamenlijk opstellen van dergelijke richtlijnen kan worden gebruikgemaakt van praktijkervaringen, zodat een doeltreffende richtlijn ontstaat die ook uitvoerbaar is.

De PI-richtlijnen worden in werkgroepverband ontwikkeld onder auspiciën van een bestuurslid in de rol van projectleider. Deze ziet er onder meer op toe dat de PI-kwaliteitsrichtlijnen door de werkgroep worden gehandhaafd. De deelnemers van de werkgroepen zijn primair afkomstig uit de organisaties die aangesloten zijn bij PI, maar niet uitsluitend. Het betreft beveiligingsfunctionarissen en ICT-auditors van uiteenlopende bedrijven en instellingen, die zich kenmerken door de hoge eisen die zij in hun adviesen controlewerkzaamheden aan organisaties moeten stellen in verband met de sterke automatiseringsgraad en de belangen die met de geautomatiseerde informatievoorziening zijn gemoeid. Door deze achtergrond vormen de deelnemers een representatieve afspiegeling van de aanwezige ICT-beveiligingsexpertise in Nederland en bieden zij een draagvlak om gezag te verlenen aan de ontwikkelde richtlijnen, hetgeen bevorderlijk is voor de acceptatie door het algemene en het ICT-management.

De PI-beveiligingsrichtlijnen zijn primair bedoeld voor functionarissen die zijn belast met het implementeren van ICT-systemen, zoals systeembeheerders en technische ontwerpers en bouwers.

Daarnaast zijn de richtlijnen van betekenis voor de volgende doelgroepen.

– ICT-beveiligingsfunctionarissen (security officers en administrators). De ICT-beveiligingsfunctie binnen een organisatie is verantwoordelijk voor het (doen) treffen van beveiligingsmaatregelen. De richtlijnen bieden hierbij ondersteuning.
– ICT-management. Het ICT-management is (eind)verantwoordelijk voor de informatiebeveiliging binnen zijn competentiegebied en geeft hieraan invulling door het (doen) analyseren van risico's en het bepalen van (globale) beveiligingsdoelstellingen. De beargumenteerde keuzen in de richtlijnen zijn hierbij een handvat.
– ICT-auditors. De richtlijnen kunnen worden gehanteerd als toetsingsnorm bij ICT-audits.

Aldus bieden de richtlijnen enerzijds een handreiking aan beveiligingsfunctionarissen en het ICT-management om een toereikende en evenwichtige beveiliging van de informatievoorziening te implementeren en bieden zij anderzijds een basis aan ICT-auditors voor de normstelling bij de beoordeling van de beveiliging van een ICT-systeem.

Aan deze PI-studie hebben de volgende personen en organisaties hun medewerking verleend:
B. Bokhorst RE RA, Belastingdienst/Centrum voor ICT
R. Kuiper, Logica CMG
S. Mekking, Kadaster
Drs. P. Mercera, Hewlett Packard
Ir. J. Schapink RE, EDP Audit Pool
Drs. R. Torabkhani, UWV

Dank voor hun constructieve bijdragen in de reviewfase van de PI-studie is verschuldigd aan:
H. Luiijf, TNO-FEL
W. Tewarie, Defensie Accountantsdienst
B. de Backker, Atos/Origin
L. van Rij en J. Speckkamp, KPMG-IRM
M. Huijbers, PinkRoccade

Inhoud