Nationale Richtlijn

Toegangsbeheer

2015 - 2020

Versie 1.0 (19 november 2015)

Vereniging Beveiligingsprofessionals Nederland

ASIS INTERNATIONAL Benelux Chapter

Inhoudsopgave

1 Inleiding

Voor u ligt de eerste versie van de Nationale Richtlijn Toegangsbeheer. De Themagroep Fysieke Beveiliging van de Vereniging Beveiligingsprofessionals Nederland heeft, in samenwerking met vertegenwoordigers van de ASIS International Benelux Chapter, deze Nationale Richtlijn opgesteld. Aanleiding om deze richtlijn op te stellen was het feit dat er in de praktijk nog steeds veel onbeantwoorde vragen zijn over het geheel van toegangsbeheersingsmaatregelen waarmee aan personen en goederen de toegang tot een organisatie gegeven of ontzegd kan worden.

Uitgangspunt is dat een security professional met deze richtlijn in handen in staat is om op een transparante wijze veiligheidsnormen op te stellen voor (fysieke) toegangsverleningsmaatregelen en toegangscontrolemaatregelen. Deze Nationale Richtlijn is een eerste document uit een serie van in totaal vier procesbeschrijvingen. De komende jaren zal de Themagroep Fysieke Beveiliging ook nog richtlijnen voor Toezicht, Alarmverificatie en Incidentmanagement gaan opstellen.

Aan de totstandkoming van deze Nationale Richtlijn Toegangsbeheer hebben de onderstaande personen, medewerking gegeven:

- Ronald Eygendaal, Croon Elektrotechniek;
- Ed Komduur, Pinkerton EMEA;
- Raimond Pronk, Rotterdam The Hague Airport;
- Jan van Twillert CPP CSP, Orca Secure.

Daarnaast hebben ook leden van de Vereniging Beveiligingsprofessionals Nederland en de ASIS International Benelux Chapter tijdens de reviewperiode commentaar gegeven.

Doelstelling van deze Nationale Richtlijn is dat u als security professional met dit document in handen een leidraad heeft die u behulpzaam kan zijn bij het effectief en transparant inzetten van het instrument toegangsbeheer. Bij het opstellen van deze richtlijn is, in het kader van herkenbaarheid en eenduidigheid, gekozen voor een zelfde structuur zoals ook gebruikt is bij de Nationale Richtlijn Pre-employment en In-employment Screening en de Nationale Richtlijn Protective Intelligence.

Het document is een levend document en zal regelmatig van updates worden voorzien, in de vorm van bijlagen, naar aanleiding van ‘ronde-tafel-sessies’ met experts waarbij specifieke onderdelen van deze richtlijn verder worden uitgewerkt.

Berndt Rif MSc MBA CPP
Voorzitter Themagroep Fysieke Beveiliging

2 Definitie

Het is belangrijk om in de procesbeschrijving Toegangsbeheer een duidelijke omschrijving van het begrip op te nemen. Het zal duidelijk moeten zijn waarvoor het proces wordt ingezet (reikwijdte) en waarvoor het proces niet wordt ingezet (uitsluitingen). In de volgende drie paragrafen worden voorbeelduitwerkingen gegeven.

VOORBEELDUITWERKING

2.1 Omschrijving

Het proces dat het mogelijk maakt om (met de daartoe benodigde middelen) personen, voertuigen, stoffen en goederen op vastgestelde tijden doorgang te verlenen of te ontzeggen tot zones, compartimenten of personen, evenals het weren van het binnendringen van zones of compartimenten.

2.2 Scope

Het proces Toegangsbeheer wordt ingezet om:

- *Personen, voertuigen, stoffen en goederen de toegang tot compartimenten te ontzeggen waarvoor zij een (mogelijk) risico zouden kunnen vormen*
- *personen, voertuigen, stoffen en goederen de toegang tot personen, systemen en processen te ontzeggen waarvoor zij een (mogelijk) risico voor de veiligheid kunnen vormen;*
- *tegen te gaan dat goederen onbevoegd worden meegenomen of toegevoegd;*
- *te ontmoedigen dat informatie onbevoegd wordt meegenomen of toegevoegd;*

2.3 Uitsluitingen

- *(Logische) toegangsbeveiligingsmaatregelen die worden geïmplementeerd op basis van het informatiebeveiligingsbeleid van de organisatie*
- *(Fysieke) toegangsbeveiligingsmaatregelen van tijdelijke aard voor reizen en evenementen*
- *(Fysieke) toegangsbeveiligingsmaatregelen met een ad hoc karakter naar aanleiding van een (nieuw) onderkende dreiging*

3 Doelstelling

Het is belangrijk om in de procesbeschrijving Toegangsbeheer een duidelijke omschrijving van de doelstelling van het proces op te nemen. Hieronder volgt een voorbeeld van een mogelijke doelstelling.

VOORBEELD UITWERKING

De doelstelling van het proces Toegangsbeheersing is:

- *het gecontroleerd toegang verlenen aan personen, voertuigen, stoffen en goederen zodat niet geaccepteerde risico's manifest kunnen worden;;*
- *inzicht te hebben wie binnen <NAAM ORGANISATIE> in welke zone, of indien voorgeschreven, in welk compartiment aanwezig is of aanwezig is geweest.*

4 Beleidsbasis

Het is belangrijk om in de procesbeschrijving Toegangsbeheer een duidelijke relatie te leggen met het door de organisatie vastgestelde beleid. Hieronder volgt een voorbeeld van een mogelijk op te nemen verwijzing.

VOORBEELD UITWERKING

Het proces Toegangsbeheer vindt haar oorsprong in de ‘’Business Code of Ethics” of “Business Principles” en het Beleidsplan Beveiliging <NAAM ORGANISATIE>, te weten in hoofdstuk XXX:

Overeenkomstig het gestelde in het Beleidsplan Beveiliging <NAAM ORGANISATIE> zijn de dreigingen die voortkomen uit de vastgestelde risicoanalyse, vertaald in beveiligingsdoelstellingen en het daarbij behorende weerstandsniveau (zie document XXX).

Op welke wijze het proces Toegangsbeheer een bijdrage dient te geven aan het creëren van voldoende weerstand tegen de onderkende (be)dreigingen blijkt uit de door de directie vastgestelde tactische kader (zie hoofdstuk 5).

5 Tactisch kader

Het is belangrijk om in de procesbeschrijving Toegangsbeheer uitgangspunten op te nemen waaraan de organisatie zich gecommitteerd heeft. Dit voorkomt vragen met betrekking tot taken, verantwoordelijkheden en bevoegdheden. Ook is het belangrijk om vast te leggen welke kaders noodzakelijk zijn om het proces goed te kunnen uitvoeren en deze kaders nader uit te werken in specifieke documenten. In de volgende twee paragrafen worden voorbeelden gegeven.

VOORBEELD UITWERKING

5.1 Tactische uitgangspunten

- *Binnen <NAAM ORGANISATIE> vindt zonering en compartimentering plaats;*
- *bedrijfsprocessen zijn, naar aanleiding van de risicoanalyse, op basis van criteria voor beschikbaarheid, integriteit en vertrouwelijkheid ingedeeld binnen een zone;*
- *voor elke zone, en in sommige gevallen voor compartimenten, zijn eisen gesteld ten aanzien van toegankelijkheid (inclusief fysieke weerstand van de schil), toegangsverlening, mogelijkheid tot meelopen en het uitvoeren van controles;*
- *het aantal doorgangen is tot een minimum beperkt (op basis van het ambitieniveau van zowel security als safety);*
- *doorgangen zijn gesloten tenzij er een functionele reden is om deze te openen;*
- *autorisaties worden uitsluitend toegekend aan personen van wie de betrouwbaarheid in voldoende mate is vastgesteld;*
- *autorisatie worden op compartimentniveau afgegeven, waarbij het functioneel ´need to be´ principe leidend is;*
- *de stromen publiek, bezoekers en medewerkers zijn waar mogelijk van elkaar gescheiden;*
- *bezoekers worden pas toegelaten na verificatie van de identiteit, registratie van het bezoek en na de vaststelling dat er van de bezoeker geen dreiging uitgaat;*
- *het verlenen van toegang vindt, waar mogelijk, geautomatiseerd plaats zonder interventie van de mens;*
- *de weerstand van de buitenschil is zodanig dat dreigingen daar zoveel mogelijk worden tegengegaan, opdat daarmee de bedrijfsprocessen binnen <NAAM ORGANISATIE> niet onnodig door overgangen tussen zones worden belemmerd;*
- *de integraal lijnmanager is verantwoordelijk voor het vaststellen van wie voor welk gebied, waarvoor de lijnmanager verantwoordelijk is, geautoriseerd worden.*
- *toegangsautorisaties aan personeelsleden of daaraan gelijkgestelden worden pas verstrekt nadat, door middel van een preemployment screening, is vastgesteld dat er geen dreiging van de betreffende persoon uit gaat*

5.2 Uitwerking in documenten

De uitwerking van de bovengenoemde tactische beleidsuitgangspunten komt terug in de volgende documenten (niet limitatief):

- *Zoneringsmethodiek;;*
- *veiligheidsnormen zonering;*
- *cameraplan;*
- *functionele programma´s van eisen*

- *werkinstructies*

6 Procesbeschrijving

Het is belangrijk om in de procesbeschrijving Toegangsbeheer duidelijk aan te geven uit welke deelprocessen het bestaat. Tevens zal duidelijk moeten zijn:

- welke input nodig is voor het uitvoeren van een specifieke processtap;
- welke output het resultaat is van een processtap en
- wat het (rest)risico is als de processtap wordt overgeslagen.

Ook zal duidelijk moeten zijn:

- wat de doelstelling van een processtap is;
- welke relaties er bestaan met andere beveiligingsprocessen en
- wie er voor de uitvoering van welke (deel)activiteit verantwoordelijk is.

In de volgende zes paragrafen worden voorbeelden gegeven van een mogelijke uitwerking. In de bijlage is een schematisch overzicht van de totale procesbeschrijving gevoegd.

VOORBEELD UITWERKING

6.1 Opdeling in deelprocessen

Het proces Toegangsbeheer is opgedeeld in de navolgende deelprocessen:

1. *Tactische kaders bepalen*
2. *Toegangsmaatregelen implementeren en onderhouden*
3. *Toegangs(verlenings)middelen beheren*
4. *Toegang verlenen/weigeren*
5. *Rapporteren*

Hieronder volgt een beschrijving van de deelprocessen.

6.2 Deelproces 1: Tactische kaders bepalen

6.2.1 Doel

Op hoofdlijnen bepalen op welke wijze het proces Toegangsbeheer wordt vormgegeven en welke kaders daarvoor noodzakelijk zijn.

6.2.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.2.3 Input

- *Mission statement, Business Principles, Business Code of Conduct.*
- *Beveiligingsbeleid < naam organisatie>.*
- *Vastgestelde risicoanalyse <naam organisatie>.*

6.2.4 Stappenplan

Activiteit	Toelichting	Verantwoordelijk
Opstellen tactische uitgangspunten fysieke beveiliging	*Er kan gekozen worden om een baseline van beveiligingsmaatregelen te implementeren op basis van algemeen geaccepteerde normen (bijvoorbeeld ISO)*	
Uitwerken tactische uitgangspunten in; - *Zoneringsmethodiek* - *Beveiligingsnormen* - *Maatregelmix zonering*		
Vaststellen tactische uitgangspunten fysieke beveiliging		

6.2.5 Output

- *Geactualiseerde en vastgestelde tactische uitgangspunten*
- *Zoneringsmethodiek*
- *Beveiligingsnormen*
- *Maatregelmix*

6.2.6 Relaties

- *Proces Risicoanalyse*
- *Operationele Beveiligingsprocessen (Toezicht, Alarmverificatie en Incidentmanagement.)*

6.2.7 Restrisico's

- *Indien in het beveiligingsbeleid en in het beveiligingsplan geen of onvoldoende door de portefeuillehouder geaccordeerde waarborgen zijn opgenomen voor de inzet van het instrument Toegangsbeheer, zal dit instrument niet effectief kunnen worden ingezet.*
- *Indien de baseline van geïmplementeerde beveiligingsmaatregelen gebaseerd is op algemeen gehanteerde en geaccepteerde (ISO) normen, en niet voortkomt uit een specifieke risicoanalyse voor de eigen organisatie, dan is er geen relatie tussen de onderkende capaciteit en motivatie van aanvallers en de getroffen beveiligingsmaatregelen.*

6.3 Deelproces 2: Toegangsmaatregelen implementeren en onderhouden

6.3.1 Doel

Bepalen, implementeren en onderhouden van de maatregelen die het mogelijk maken om toegang te verlenen of om toegang te weigeren.

6.3.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.3.3 Input

- *Tactische uitgangspunten*
- *Zoneringsmethodiek*
- *Beveiligingsnormen*
- *Maatregelmix*

6.3.4 Stappenplan

Activiteit	**Toelichting**	**Verantwoordelijk**
Bepalen OBE-maatregelen	*Maatregelen dienen te voldoen aan het tactische kader en dienen te worden vastgelegd*	*Beveiliging*
		Facilitaire dienst

6.3.5 Output

- *Vlekkenplan*
- *Sluitplan*
- *Programma van Eisen Toegangscontrole Systeem*
- *Programma van Eisen Fysieke Beveiligingsmaatregelen*

6.3.6 Relaties

- *Proces Risicoanalyse*
- *Operationeel beveiligingsproces Toezicht, Alarmverificatie.*

6.3.7 Restrisico’s

- *X*

6.4 Deelproces 3: Toegangs(verlenings)middelen beheren

6.4.1 Doel

Het beheren en uitgeven van toegang(verlenings)middelen zodat elk persoon toegang kan krijgen tot de zones en/of compartimenten waar hij/zij op vooraf bepaalde tijdstippen toegangsrechten voor heeft

6.4.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.4.3 Input

- *Vlekkenplan*
- *Sluitplan*
- *Zoneringsmethodiek*

6.4.4 Stappenplan

Activiteit	***Toelichting***	***Verantwoordelijk***
Opstellen van een autorisatiematrix op basis van vastgestelde functieprofielen	*Primair proces verantwoordelijke geeft aan wie waar op basis functionele noodzakelijkheid autorisatie krijgt*	*Lijnmanagement*
Opstellen van een exclusiematrix op basis van functiescheiding		*Lijnmanagement*

6.4.5 Output

- *Autorisatiematrix*
- *Exclusiematrix*

6.4.6 Relaties

- *Proces Risicoanalyse*

6.4.7 Restrisico’s

- *X*

6.5 Deelproces 4: Toegang verlenen/weigeren

6.5.1 Doel

Het daadwerkelijk doorgang verlenen of ontzeggen van personen, goederen en/of informatie

6.5.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.5.3 Input

- *Verzoek tot verlenen van doorgang*

6.5.4 Stappenplan

Activiteit	***Toelichting***	***Verantwoordelijk***
Verzoek toegang ontvangen		
Controle	*Tijdstip, autorisatie, veiligheid, goederen, antipassback, meelopen*	*TCS of Beveiliger*
Doorgang verlenen of weigeren		*TCS of Beveiliger*

6.5.5 Output

- *Rapportage over*
  - *Weigeringen (personen, goederen)*
  - *Incidenten (meelopen, antipassback)*
  - *Veiligheid*

6.5.6 Relaties

- *Proces Risicoanalyse*

6.5.7 Restrisico's

- *X*

6.6 Deelproces 5: Rapporteren

6.6.1 Doel

Het verstrekken van managementinformatie over het proces Toegangsbeheer

6.6.2 Verantwoordelijk

De <naam functionaris> van <naam organisatie>, namens deze de afdeling <naam afdeling>.

6.6.3 Input

- *Rapportage deelproces Toegang verlenen/weigeren*
-

6.6.4 Stappenplan

Activiteit	Toelichting	Verantwoordelijk
Het opstellen van management informatie op basis van input uit voorgaande deelprocessen		

6.6.5 Output

- *Managementrapportage*

6.6.6 Relaties

- *Proces Risicoanalyse*

6.6.7 Restrisico's

- *X*

7 Operationele randvoorwaarden

Het is belangrijk om in de procesbeschrijving Toegangsbeheer op te nemen over welke competenties functionarissen moeten beschikken om de proceswerkzaamheden goed te kunnen uitvoeren. Ook zal duidelijk moeten zijn welke systemen functionarissen voor de uitvoering van de werkzaamheden ter beschikking moeten staan en welke (werk)instructies noodzakelijk zijn.

7.1 Competenties

Bij het vaststellen van de benodigde competenties is het belangrijk om er bij het bepalen van competenties rekening mee te houden dat bij het proces Toegangsbeheer betrokken personen zich staande moeten kunnen houden in complexe besluitvormingsprocessen waar men zowel juridische consequenties alsook gevolgen op beveiligingsvlak moet overzien. Tevens is een hoge mate van flexibiliteit, organisatie sensitiviteit en omgevingssensitiviteit noodzakelijk. Een individu die werkzaam is op het vlak van Toegangsbeheer kan zijn of haar werkzaamheden binnen de noodzakelijk op te zetten en te onderhouden netwerken alleen uitvoeren als hij of zij door externe gesprekspartners als betrouwbaar, integer en kundig wordt ervaren.

7.2 Systemen

De Toegangsbeheer professional dient op een systematische wijze historie, trends en ontwikkelingen te kunnen vastleggen. Tevens dient deze professional de beschikbare gegevens op een transparante en controleerbare wijze te kunnen analyseren. Dit zijn de uitgangspunten bij het identificeren van noodzakelijke ondersteunende systemen.

7.3 Documenten

Voor een efficiënte en deugdelijke operationele werking van het proces Toegangsbeheer zijn vastgestelde protocollen en werkinstructies noodzakelijk. Alleen dan kan aan de eis van transparantie en herleidbaarheid worden voldaan. Iedere organisatie zal zelf moeten bepalen, uitgaande van het eigen kwaliteitsmanagementsysteem, wat de minimaal benodigde protocollen en werkinstructies zijn.

8 Kwaliteitsborging

Het is belangrijk om in de procesbeschrijving Toegangsbeheer een paragraaf op te nemen waarin normen en indicatoren staan beschreven. Dit om achteraf te kunnen vaststellen of het proces goed is uitgevoerd. Teneinde misverstanden te voorkomen, zal tevens beschreven moeten worden op welke wijze meting zal plaatsvinden.

8.1 Norm

Er kan pas worden vastgesteld of er voor het proces Toegangsbeheer sprake is van een voldoende niveau indien normen SMART geformuleerd zijn. Tevens dient er, bij de inrichting van het proces, sprake te zijn van een gesloten kwaliteitscirkel.

8.2 Indicator

In het benoemen van indicatoren is het belangrijk om te bepalen wat het verschil is tussen de geïdentificeerde BRUTO-dreiging (output proces Toegangsbeheer en input proces Risicoanalyse) en de vastgestelde NETTO-dreiging (output proces Risicoanalyse en input tactische beveiligingsprocessen).

8.3 Meting

Meting is alleen mogelijk als voldaan is aan de eis van SMART geformuleerde normen en daarvan afgeleide normen.

9 Begrippenlijst in het kader van deze Richtlijn

Proces Alarmverificatie	Het proces dat het mogelijk maakt om (met de daartoe benodigde middelen) (alarm)meldingen die afkomstig zijn vanuit het proces Toezicht te ontvangen, te beoordelen en afhankelijk van de gestelde diagnose af te handelen.
Autorisatiematrix	Een matrix bestaande uit autorisatieprofielen en functieprofielen. In de matrix wordt zichtbaar gemaakt welk functieprofiel op basis van functionele noodzaak autorisatie ontvangt voor zoneovergangen, gebieden, compartimenten.
Beveiligingsnormen	Specifieke normen ten aanzien van (zone) overgangen, gebieden of compartimenten op het gebied van; - toegangsverlening - identificatie - weerbaarheid - meelopen
Cameraplan	Een plan waarin is vastgelegd: - waar camera's zijn gepositioneerd; - het specifieke doel van een camera - type camera - zichtlijnen en schaduwgebieden - configuratie van parameters zoals openingshoek, richting, hoogte etc.
Detectieplan	Een plan waarin is vastgelegd waar en met welke middelen detectie van onregelmatigheden plaatsvindt.
Exclusiematrix	Een matrix waarin op basis van functiescheiding is vastgesteld waar geen autorisatie aan mag worden toegekend.
Proces Incidentmanagement	Het proces dat ervoor zorgt dat (met de daartoe benodigde middelen) een incident zo snel mogelijk beheersbaar wordt. Het proces dient ook te zorgen voor een terugkeer naar een veilige situatie en het treffen van herstel maatregelen.
Maatregelmix	Een mix van Organisatorische, Bouwkundige en Elektronische maatregelen en de onderlinge samenhang van de maatregelen
Sluitplan	Een plan waarin is vastgelegd met welke middelen doorgangen zijn gesloten.
Tactische Uitgangspunten	Uitgangspunten welke op tactische niveau zijn vastgelegd met het doel om demarcatie tussen bevoegdheden en verantwoordelijkheden te bepalen.
Proces Toegangsbeheer	Het proces dat het mogelijk maakt om (met de daartoe benodigde middelen) personen, stoffen en goederen op vastgestelde tijden doorgang te verlenen of te ontzeggen tot zones, compartimenten of personen, evenals het weren van het binnendringen van zones of compartimenten.
Toegangscontrole	Het verlenen van toegang aan personen tot de organisatie op basis van een toegangsverleningsmiddel en een

	controle of de persoon de juiste gebruiker van het toegangsverleningsmiddel is.
Proces Toezicht	Het proces dat het mogelijk maakt om (met de daartoe benodigde middelen) enerzijds (mogelijke) risicovolle situaties waar te nemen, anderzijds vast te stellen dat veiligheidsnormen worden overschreden.
Vlekkenplan	Het vlekkenplan maakt inzichtelijk welke eenduidige bedrijfsprocessen waar plaatsvinden.
Zoneringsmethodiek	Een methodiek waarin op basis van de risicoanalyse is vastgesteld welke bedrijfsprocessen in welke zone dienen plaats te vinden en aan welke criteria de verschillende zoneovergangen moeten voldoen.