Vlaanderen
is wegen en verkeer

Standaardbestek 270

DEEL II

Hoofdstuk 48d

Telematica security

INHOUDSOPGAVE

1. Scope

Dit hoofdstuk beschrijft de verschillende beveiligingsvereisten die door de aanbestedende overheid worden opgelegd aan de inschrijver. Deze vereisten focussen zowel op (technische) documentatie alsook op (netwerk-) technische standaarden en logische toegangsbeveiligingsmaatregelen.

1. ICT- en informatiebeveiligingsbeleid

Het Agentschap Wegen en Verkeer beschikt over een ICT- en informatiebeveiligingsbeleid waaraan de opdrachtnemer dient te voldoen. Het beleid kan aangevraagd worden bij de opdracht gevende overheid.

2. Specifieke beveiligingsmaatregelen

2.1. Toepassingen

Elke toepassing dient minimaal volgende technieken te ondersteunen:

- op vlak van server-to-server communicatie:
    - Ondersteuning van netwerk authenticatie (IEEE802.1x): 802.1x is een IEEE standaard die de authenticatie van eindpunten regelt. De standaard maakt gebruikt van het EAPOL protocol (EAP over LAN) en is bruikbaar over zowel draadloze als bekabelde netwerken. Het is verplicht een sterke (wederzijdse) authenticatie methode te gebruiken, minimaal PEAP met EAP-TLS
    - Encryptie van de communicatie:
        - Minimaal TLS met een op AES-256 bit gebaseerd cypher;
        - Ondersteuning voor https bij het gebruik van webapplicaties.
- Koppeling van de applicatie met de LDAP infrastructuur van de aanbestedende overheid
    - De koppeling met de LDAP infrastructuur van de aanbestedende overheid is verplicht voor alle voor de aanbestedende overheid op maat ontwikkelde softwaretoepassingen (ook client-side, betreft geen PLC's), alsook voor alle servers op het niveau van het operating system
    - Het systeem (applicatie en/of server) zal erop voorzien zijn te kunnen koppelen met een primaire alsook met een secundaire LDAP server

2.2. Gebruikersrechtenbeheer

- Elk eindpunt dient afgeschermd te zijn door middel van een wachtwoord. Dit wachtwoord dient op gemakkelijke wijze aanpasbaar te zijn. Verder dient de opdrachtnemer voor elk apparaat dat aan het netwerk wordt gekoppeld, te beschrijven wat de mogelijkheden zijn inzake wachtwoordbeveiliging en eventuele scheiding van rollen en verantwoordelijkheden.
- Wat betreft servers, dient te worden voldaan aan volgende vereisten:
    - De wachtwoordpolicy van de aanbestedende overheid is integraal van toepassing op de opdracht. De wachtwoordpolicy is aan te vragen bij de aanbestedende overheid;
    - Een duidelijke opdeling in rollen en verantwoordelijkheden dient weergegeven te worden in matrix-vorm. Het toevoegen en verwijderen van rollen en autorisaties dient mogelijk te zijn. Volgende rollen dienen minimaal voorzien te zijn;
        - Operator

          Operatoren of bedienaars zijn deze personen die instaan voor de dagdagelijkse bediening van de toepassing.
        - Onderhoudstechnieker

          Het technische personeel heeft in principe dezelfde rechten als operatoren. Enkel

hebben zij extra rechten om procesvariabelen in verband met technische aspecten te wijzigen.

- (Systeem-)beheerder
  De systeembeheerder heeft onbeperkte rechten. M.a.w. de systeembeheerder kan het (visualisatie)systeem afsluiten en aanpassen en gebruikers aanmaken.
- Onbemand
  Onbemand is een waarnemend profiel zonder enige gebruiks- of bedieningsrechten.

  - Logging: Het in -en uitloggen van alle profielen wordt geregistreerd. Ook mislukte pogingen tot inloggen worden geregistreerd, maar hierbij wordt de gebruikersnaam niet gelogd. Volgende gegevens worden hierbij geregistreerd:
    - Gebruikersnaam (niet bij mislukte pogingen tot inloggen);
    - Datum & tijd van inloggen en uitloggen;
    - IP-adres van waaruit in- en uitgelogd werd.
  - Na een instelbare tijd van inactiviteit dient een bedienaar uitgelogd te worden uit de applicatie.

- De opdrachtnemer beschrijft een beheersproces dat als doel heeft dat er geen mogelijkheid bestaat dat niet-gemachtigde personen toegang kunnen krijgen tot de toepassing of de servers (bijv.. ex-werknemers van de opdrachtnemer). Het beheersproces dient minimaal volgende elementen te bevatten:
  - Interne uit-dienst procedure opgesteld door de opdrachtnemer die ook nageleefd dient te worden
  - Review-procedure van de toegangsrechten die jaarlijks uitgevoerd zal worden en die tot doel heeft de mogelijks gemaakte menselijke fouten te corrigeren
  - Procedure te volgen door de aanbestedende overheid die deze laatste in staat stelt een overzicht te krijgen van alle gebruikers en hun rollen (eindgebruikers alsook system-administrators en andere rollen).

2.3. Algemene opzet en onderhoud van het systeem

- De opdrachtnemer beschrijft een patching-politiek voor servers en eindpunten: een systeem dat niet gepatched is, is namelijk kwetsbaar voor aanvallen van binnenuit of van buitenaf.
  - De patching-politiek heeft als doel deze kwetsbaarheden te vermijden en dient minimaal rekening te houden met de volgende vereisten:
    - Patchen dient zo snel mogelijk te gebeuren;
    - Het toepassen van de patch mag geen negatieve effecten hebben op de functionaliteit (test-procedure). Ook zal de patching eerst doorgevoerd worden op het test systeem alvorens de patch toe te passen in productie. De procedure dient hierin te voorzien;
    - een noodprocedure wordt voorzien voor onmiddellijke beveiligingsnoden (voorbeelden uit het verleden in dit kader zijn Heartbleed, Shellshock, …).
  - De opdrachtnemer kan zijn procedure, indien gewenst, ook baseren op een risico-analyse. De risico-analyse zal dan op geregelde tijdstippen uitgevoerd worden en zo de pachting-noden aan het licht brengen op basis waarvan, in overleg met de aanbestedende overheid, de gepaste acties kunnen genomen worden;
  - De aanbestedende overheid behoudt zich het recht voor een vulnerability scan uit te voeren bij wijze van verificatie van de patching-politiek van de opdrachtnemer.

- De inschrijver voorziet in een gescheiden omgeving voor test en productie. De test omgeving dient ten allen tijde een exacte functionele kopie te zijn van de productie omgeving behalve in vooraf afgesproken test periodes waarin de functionele opzet kan verschillen. Na de test periodes dient de test omgeving telkens bijgewerkt te worden tot ze de productie omgeving weerspiegelt.
    - Er is sprake van een exacte functionele kopie, wat wil zeggen dat de test omgeving toch nog kan verschillen van de productie omgeving. Dit kan bijvoorbeeld op het vlak van redundantie of op het inzetten van minder performante servers aangezien een test omgeving over het algemeen minder belast wordt dan een productie omgeving.

2.4. Toegang vanop afstand tot het Telematica Netwerk

De aanbestedende overheid beschikt over een aanvraagformulier en bijhorende aansluitingsvoorwaarden voor toegang vanop afstand tot het “Telematica Netwerk” [TN]. Indien toegang vanop afstand noodzakelijk is, worden deze documenten aangeleverd door de beheerder van het TN. Indien de gebruiker vanuit een netwerk dat niet in het beheer ligt van Agentschap Wegen en Verkeer toegang wil tot het TN, zal de eindgebruiker, m.b.v. VPN technologie, toegang krijgen tot een vooraf gedefinieerd gedeelte van het TN. Deze toegang vanop afstand wordt opgezet met gebruik van een SSL-VPN technologie. Enkel door de beheerder van het TN goedgekeurde SSL VPN software is toegestaan, dewelke kan gevonden worden in de aansluitingsvoorwaarden voor toegang vanop afstand tot het TN, aangeleverd door de beheerder van het TN. De aansluitingsvoorwaarden kunnen aangevraagd worden na gunning van het bestek. Alle andere technologieën/software (bv. Teamviewer, …) voor toegang vanop afstand wordt verboden, tenzij met expliciete goedkeuring van de beheerder van het TN.

De gebruiker dient de door de beheerder opgelegde aansluitingsvoorwaarden voor toegang vanop afstand ten alle tijden te respecteren.

De opdrachtnemer is verplicht een lijst op te stellen waarin alle werknemers, die gebruik maken van de toegang vanop afstand, zijn vermeld met bijhorende IP adressen tot dewelke deze werknemers toegang hebben. Elke wijziging in deze lijst dient gecommuniceerd te worden naar de leidend ambtenaar van het bestek en de beheerder van het TN. De opdracht gevende overheid behoudt zich het recht voor ten alle tijden de correctheid van de lijst te contoleren.

Bij het beëindigen van de aanneming zal in overleg met de leidend ambtenaar van het bestek en de beheerder van het TN een datum vooropgesteld worden waarop alle toegang vanop afstand voor de opdrachtnemer zal opgeheven worden.

2.5. Netwerkverbinding naar het Telematica Netwerk

Elk apparaat dat gekoppeld is met het Telematica Netwerk mag slechts een enkele netwerkverbinding hebben, namelijk deze met het TN. Elke afwijking van deze veiligheidsvereiste kan enkel uitgevoerd worden met expliciete goedkeuring van de beheerder van het TN.

Hoofdstuk 48d werd opgemaakt door:

Voorzitter

Gregory Boeckmans

Leden van de werkgroep

Jan Van Boxelaere, Jeroen Avau, Koen Wardenier, Jurgen Latte, Ben Geerts, Jos Hennissen, Stanny Van Herzeele, Peter Lewyllie.

Colofon

Verantwoordelijke uitgever :
ir. Tom Roelants
administrateur-generaal

Contactadres :
Afdeling Expertise Verkeer en Telematica
Koning Albert II-laan 20, bus 4
1000 BRUSSEL

Tel. 02-553 78 02

www.wegenenverkeer.be - expertise.verkeer.telematica@mow.vlaanderen.be

Depotnummer :
D/2017/3241/125