Requirements Beveiligbaarheid (Security) v2.5

Requirements aan de centrale BRP voorziening inclusief migratiecomponenten zijn opgedeeld volgens ISO 25010.

Definitie

De mate waarin een product of systeem informatie en gegevens beschermt zodat personen, andere producten of systemen de juiste mate van gegevenstoegang hebben passend bij hun soort en niveau van autorisatie.

- Vertrouwelijkheid (Confidentiality)
  De mate waarin een product of systeem er voor zorgt dat gegevens alleen toegankelijk zijn voor diegenen die geautoriseerd zijn.
- Integriteit (Integrity)
  De mate waarin een systeem, product of component ongeautoriseerde toegang tot of aanpassing van computerprogramma's of gegevens verhindert.
- Onweerlegbaarheid (Non-repudiation)
  De mate waarin kan worden bewezen dat acties of gebeurtenissen plaats hebben gevonden, zodat later deze acties of gebeurtenissen niet ontkend kunnen worden.
- Verantwoording (Accountability)
  De mate waarin acties van een entiteit getraceerd kunnen worden naar die specifieke entiteit.
- Authenticiteit (Authenticity)
  De mate waarin bewezen kan worden dat de identiteit van een onderwerp of bron is zoals wordt beweerd.
  De mate waarin een claim over de oorsprong of de auteur van de informatie verifieerbaar is, bijvoorbeeld aan handschrift.

De requirements zijn opgedeeld in de groepen 'algemeen', 'koppelvlakken' en 'gebruikersinterface'. Aangezien de centrale BRP geen gebruikersinterface ten behoeve van reguliere gebruikers heeft, betreft die laatste groep alleen de gebruikersinterface ten behoeve van beheer van de voorziening.

Requirements algemeen

Onderstaande algemene requirements worden gesteld aan de door het project O&R op te leveren maatwerkcomponenten van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

Code	Requirement
RD-BEV-004	De volgende richtlijn wordt gehanteerd: Controleer altijd op "geldigheid" en niet op "ongeldigheid". Daarbij wordt minimaal gecontroleerd op grenswaarden, ongeldige tekens, onvolledige gegevens, gegevens die niet aan het juiste format voldoen, inconsistentie van gegevens en (buffer)lengte. Deze controles dienen te beschermen tegen SQL-injectie, buffer-overflow, crashen of vastlopen van de applicatie, verwerken buiten de gedefinieerde regels om en overschrijding van de autorisatie.

RD-BEV-006	Technische fouten en bijbehorende technische meldingen (zoals een stacktrace of melding van een extern systeem) mogen nooit zichtbaar zijn voor de eindgebruiker[1]; er mag geen info over het onderliggende of achterliggende systeem naar buiten.
RD-BEV-037	Foutmeldingen aan eindgebruikers bevatten geen persoonsgegevens, met uitzondering van persoonsgegevens die door deze zelfde eindgebruiker zijn opgegeven in een bericht waar de foutmelding op volgt.
RD-BEV-050	Gebruik voor "one-way hashes" altijd een salt.
RD-BEV-019	Voorkom het gebruik van third party libraries die niet in de repository manager staan en release builds dienen altijd alleen vanuit de repository manager hun dependencies te downloaden.
RD-BEV-023	In ieder geval de volgende gebeurtenissen binnen de (maatwerk)software worden gelogd: • Elke poging toegang te verkrijgen op het systeem (minimaal de gebruiker, de service instantie/node of netwerk of informatiesysteem, de tijd, en voor zover mogelijk de locatie (netwerkadres) van de gebruiker) • Elke niet geslaagde poging om toegang te verkrijgen • Elke storing (foutmelding) • Security fouten/alerts • Berichten die niet aan de integriteitswaarborg voldoen • Een vanuit het systeem verzonden bericht dat door de ontvanger is geweigerd • Het niet of niet juist verwerken van gegevens • Situaties waarbij de gebruiker (bijhouder) correcties moet doorvoeren om gegevens correct te laten verwerken.
RD-BEV-047	De applicaties moeten naar een ander systeem (andere machine) kunnen loggen dan het systeem waar de applicatie zelf op draait.
RD-BEV-048	Het systeem maakt het mogelijk om bepaalde logmeldingen te laten leiden tot een actieve melding aan de beheerder.
RD-BEV-025	Het systeem heeft gescheiden koppelvlakken/gebruikersinterfaces voor enerzijds beheer en anderzijds eindgebruikerstoegang zodat het systeem kan functioneren op een infrastructuur met (eventueel virtueel) gescheiden netwerken voor eindgebruikerstoegang (koppelvlakken), beheer en opslag.
RD-BEV-030	Het systeem is (voor zover van toepassing) beveiligd tegen risico's zoals benoemd in de OWASP top-10 lijst. De gehanteerde lijst mag bij oplevering maximaal 12 maanden oud zijn. In de softwaredocumentatie is per OWASP punt beargumenteerd of betreffend punt van toepassing is op de op te leveren (maatwerk)software, en indien dit het geval is, welke maatregelen zijn genomen binnen de (maatwerk)software.
RD-BEV-036	Verifieer voor een verwerking of de gebruiker (of beheerder) geautoriseerd is voor betreffende verwerking.
RD-BEV-039	Het informatiesysteem moet functies bevatten waarmee vastgesteld kan worden of gegevens correct verwerkt zijn. Hiermee wordt een geautomatiseerde controle bedoeld waarmee (duidelijke) transactie- en verwerkingsfouten kunnen worden gedetecteerd.
RD-BEV-040	Stapelen van fouten wordt voorkomen door toepassing van "noodstop" mechanismen.
RD-BEV-041	Verwerkingen zijn bij voorkeur herstelbaar zodat bij het optreden van fouten en/of

[1] Een beheerder wordt niet beschouwd als eindgebruiker.

	wegraken van informatie dit hersteld kan worden door het opnieuw verwerken van de informatie.
RD-BEV-049	Van de maatwerksoftware is gedocumenteerd welke toegang tot resources (bijvoorbeeld databases en queue's) zij vereisen zodat binnen de systeemsoftware de toegang tot deze resources kan worden beperkt tot de processen waarbinnen deze maatwerksoftware draait.
RD-BEV-032	Wachtwoorden worden nooit in originele vorm (plaintext) opgeslagen of verstuurd, maar in plaats daarvan wordt het versleutelde wachtwoord opgeslagen (bij opslag in systemen, nooit terug te herleiden naar plaintekst) Een uitzondering hierop vormt het opslaan van wachtwoorden in configuratiefiles die services binnen het systeem nodig hebben om resources te benaderen (zoals een wachtwoord om een database te benaderen). Gedocumenteerd is waar het systeem dergelijke wachtwoorden opslaat zodat bij de inrichting van de infrastructuur passende beveiligingsmaatregelen kunnen worden genomen.
RD-BEV-052	In het systeem opgenomen persoonsgegevens kunnen door de bijhouder worden gecorrigeerd.

Requirements koppelvlakken

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-026	Gebruikerstoegang anders dan via GBA koppelvlakken of BRP koppelvlakken is niet mogelijk.
RD-BEV-027	Functies voor bijhouding en voor levering zijn logisch gescheiden binnen de BRP koppelvlakken.
RD-BEV-028	Gebruikerstoegang via BRP koppelvlakken verloopt uitsluitend met berichtuitwisseling conform Digikoppeling 3.0, profielen "2W-be-s", "2W-R-S" of "osb-rm-s".
RD-BEV-029	Gebruikerstoegang via GBA koppelvlakken verloopt uitsluitend met berichtuitwisseling conform het Logisch Ontwerp GBA.
RD-BEV-042	Niet integere berichten krijgen een antwoordbericht met een standaard melding die geen inhoudelijke informatie geeft over de authenticatie en autorisatie die de stelselapplicatie uitvoert.
RD-BEV-043	De volledigheid en juistheid van de uitvoer van het systeem via de BRP koppelvlakken is vast te stellen door een digitale handtekening (of anderszins via een checksum of hash).
RD-BEV-044	De applicatie verstrekt niet meer gegevens dan de gegevens die op grond van de autorisatie mogen worden verstrekt.
RD-BEV-045	Bij een vraag aan de applicatie verstrekt de applicatie geen andere gegevens dan de gegevens die zijn gevraagd.
RD-BEV-046	Gegevens worden alleen verstrekt aan op voorhand bekende afleveradressen.
RD-BEV-013	Het systeem biedt de mogelijkheid aan de beheerder om het gebruik van het systeem via de koppelvlakken te blokkeren. De niveau’s die daarbij worden onderscheiden zijn (juridisch) geautoriseerde partij, ondertekenende partij, aangesloten partij en de toegang (de combinatie van geautoriseerde partij, ondertekenende partij, aangesloten partij en de verzameling functies die op het systeem mogen worden uitgevoerd)

Requirements (beheer)gebruikersinterface

Onderstaande requirements worden gesteld aan de koppelvlakken van de centrale BRP voorziening inclusief migratiecomponenten met betrekking tot beveiliging:

RD-BEV-018	Bij client/server applicaties dienen validaties ook altijd op de server-kant plaats te vinden.
RD-BEV-020	Beheerfunctionaliteit binnen de (maatwerk)software is verdeeld in rollen.
RD-BEV-021	Een beheerder krijgt binnen de (maatwerk)software slechts toegang tot beheerfunctionaliteit toegewezen aan één rol.
RD-BEV-022	Een beheerder wordt door de (maatwerk)software geauthentiseerd en voor maximaal één rol geautoriseerd via het IAM (Identity Access Management) systeem van de Rijksdienst voor Identiteitsgegevens.
RD-BEV-024	Er mag geen gebruik kunnen worden gemaakt van mobiele code anders binnen een web gebruikersinterface het gebruik van Javascript.
RD-BEV-031	Na het succesvol aanmelden moet de beheerapplicatie van de stelselomgeving de sessiegegevens vernieuwen.
RD-BEV-033	Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
RD-BEV-034	Er mag geen informatie (zoals bijvoorbeeld een vooraf ingevulde gebruikersnamen) getoond worden voordat een beheerder geauthenticeerd en aangelogd is.
RD-BEV-035	Een sessie van een beheerder met de beheerapplicatie is strikt gebonden aan het IP-adres en aan de user-agent (browser) van de beheerder (ter preventie Session Hijacking).