cevi
CENTRUM VOOR INFORMATICA

LOGINS

NOTA

CEVI/LOGINS EN DE GDPR

PART OF THE NRB GROUP

1 INHOUDSOPGAVE

2 INLEIDING

2.1 VOORWOORD

Iedere organisatie die privacygevoelige gegevens verwerkt, valt onder de GDPR-wetgeving die op 25 mei 2018 echt afdwingbaar is. Dat geldt dus ook voor Cevi/Logins.

In dit document komen een aantal algemene punten aan bod die duidelijk maken dat Cevi/Logins compliant werken aan de vereisten van de GDPR.

2.2 COLOFON

Cevi NV - Bisdomplein 3 - 9000 GENT
Tel. Cevi Contact Center: 09 264 07 01 - fax: 09 233 05 24
E-mail: contactcenter@cevi.be
Internet: https://www.cevi.be/
Ondernemersnummer: BE 0860.972.295

Logins NV - Generaal De Wittelaan 17 B32 - 2800 Mechelen
Tel.: 015 45 48 50 - fax: 015 45 48 89
E-mail: helpdesk@logins.be
Internet: http://www.logins.be
Ondernemersnummer: BE 0458.715.671

Ondersteuning: Informatieveiligheidscel Cevi/Logins NV

3 WETTEN EN NORMEN

Cevi is bij Koninklijk besluit van 18 juli 1985 erkend als subregionaal centrum voor het uitvoeren van opdrachten bij het Rijksregister en voor het gebruik van het Rijksregisternummer voor het beheer van bestanden. Cevi NV volgt voor zijn software strikt de richtlijnen die het opgelegd krijgt door het Rijksregister.
Binnen Cevi is er daardoor een cultuur aanwezig van verhoogde waakzaamheid inzake security. Die wordt verder ondersteund door gespecialiseerde systeem-ingenieurs en organisatorische en technische hulpmiddelen en ingrepen. De komst van GDPR grijpen we aan om dit verder op procedureel vlak uit te werken. Dit met externe, gespecialiseerde ondersteuning.

3.1 HARDWARE REDUNDANTIE

Cevi beschikt over 2 computerzalen in eigen beheer, namelijk BDP (Campus Bisdomplein, Gent) en OGS (Campus Ottergemsesteenweg, Gent), op ongeveer 3 km afstand van elkaar en verbonden via CWDM apparatuur en een dark fiber van Eandis.

* Computerzaal OGS (primair Intranet) -- failover → Computerzaal BDP (back-up Intranet)
* Computerzaal BDP (primair Extranet, Opsnet, Lesnet) -- failover → Computerzaal OGS (back-up Extranet, Opsnet)

3.1.1 Centrale Storage Infrastructuur

De storage-infrastructuur is volledig redundant uitgevoerd en is voor de productieservers zo geconfigureerd dat alle data tussen de twee sites BDP en OGS volledig synchroon gespiegeld wordt.

3.1.2 Datacom infrastructuur

LAN en WAN is volledig redundant uitgevoerd.

3.1.3 Vmware virtuele serverinfrastructuur

De Vmware virtuele serverinfrastructuur is volledig redundant uitgevoerd. In geval van een site DRP start voor de productieservers een automatische failover naar de back-upsite en zijn deze servers binnen enkele minuten weer online.

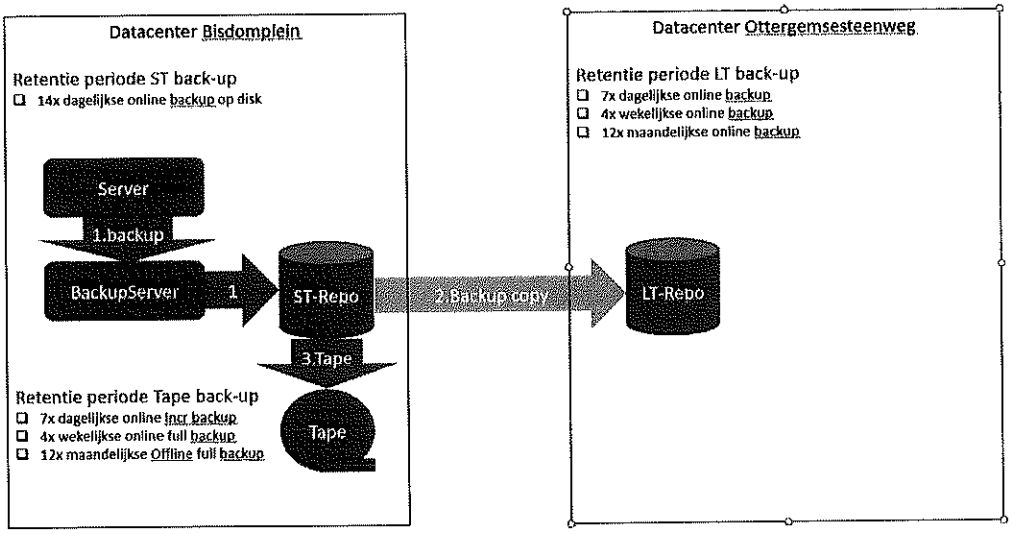
3.1.4 Back-upinfrastructuur

Voor de Virtuele server infrastructuur wordt de 3-2-1 back-upregel toegepast. Voor elke server beschikken we over minstens 3 kopieën, welke op minstens 2 verschillende type media bewaard worden en waarvan minstens 1 kopie op een andere locatie bewaard wordt. Qua retentieperiode wordt de dagelijkse back-up 14 dagen bijgehouden, de wekelijkse back-up wordt 4 weken bijgehouden en de maandelijkse back-up wordt 1 jaar bewaard.

Voor bepaalde kritische MSSQL databaseservers wordt om de 2 uur een back-up genomen met een retentieperiode van 1 dag.

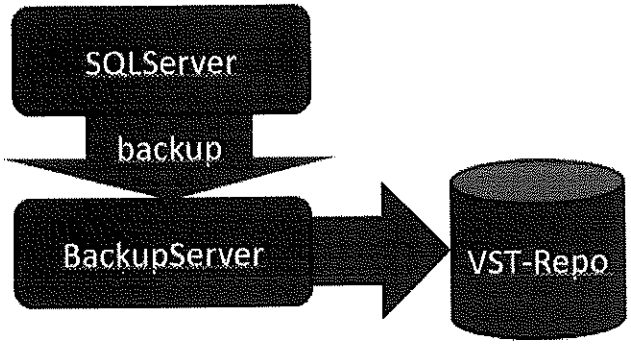
Specifiek

* Veeam Replication
  - Wordt gebruikt voor kritische infrastructuurservers
* Veeam Backup volgens de 3-2-1 regel:
  - 3 kopieën
  - 2 Verschillende media
  - 1 back-up op een andere locatie
* Veeam Surebackup:
  - Effectieve Back-up controle
* Veeam Instant recovery:
  - Asap online brengen van de back-up als VM terwijl de restore uitgevoerd wordt



Retentie periode SQL VST back-up

- 16x per 2 uur online backup



3.1.5 Netwerkschema

Er is een volledig uitgewerkt schema van de netwerkomgeving.

3.1.6 Uitval

Datacenter stroomuitval

Beschikbaarheid: elk datacenter is voorzien van een UPS = 45minuten, Vmware Geo-clustering en een script die proactief vMotion uitvoert van de virtuele servers naar de failover site.

Impact: geen tot 5 minuten offline (reboot van virtuele server).

Storage device uitval

Beschikbaarheid: Redundante SAN met RAID10 of RAID50 pools + synchrone site-mirroring.

Impact: geen

Netwerk device uitval

Beschikbaarheid: redundante LAN/WAN verspreidt over de twee datacenters.

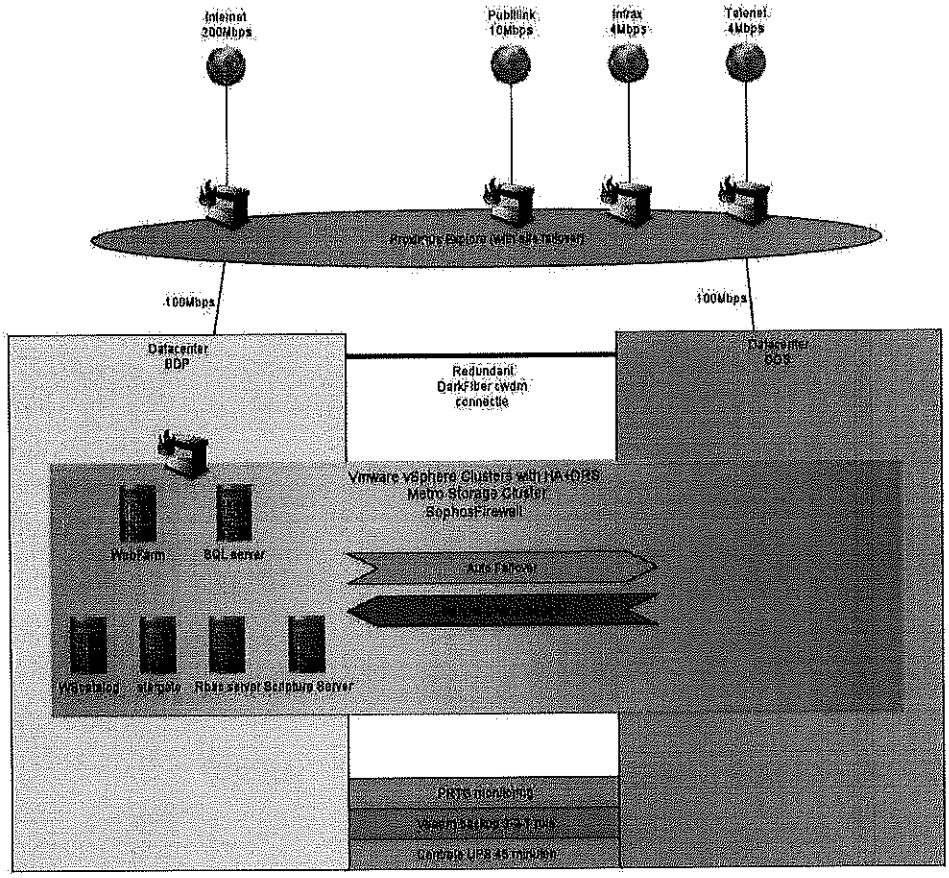
Impact: geen

Host device uitval

Beschikbaarheid: Vmware Cluster, Sophos loadbalancing

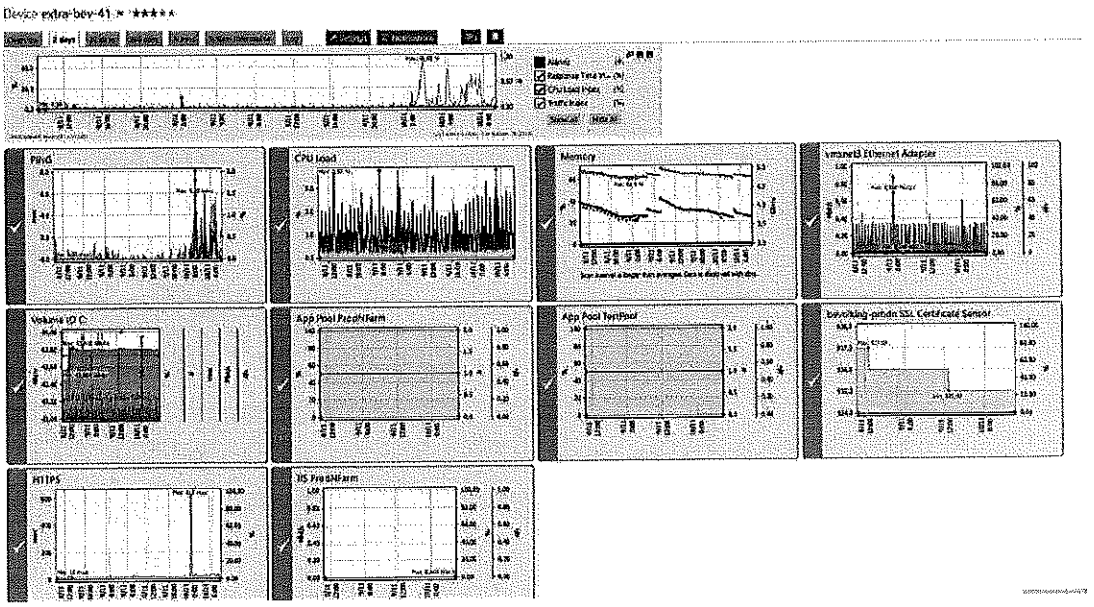
Impact: geen tot 5 minuten (reboot van virtuele server)

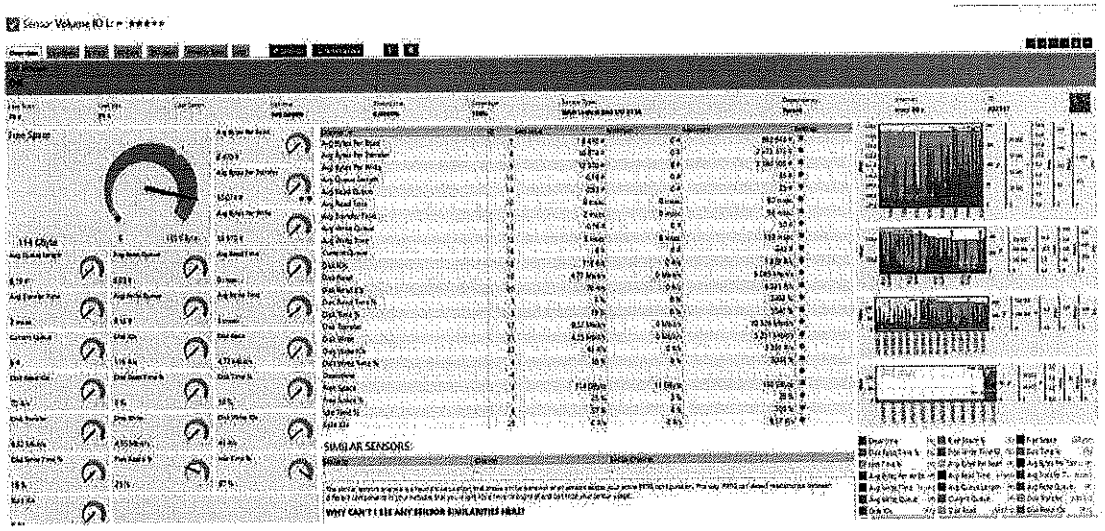
Schematisch



3.1.7 Monitoring

PRTG is het monitoringsysteem waarmee de beschikbaarheid en performantie gemonitord wordt.





3.1.8 Connectiviteit en load balancing

Klanten connecteren via een Sophos loadbalancer, de servers in de AppFarm worden verdeeld over de twee datacenters. De AppFarm kan online uitgebreid worden door het klonen van een bestaande AppFarm Server.

3.1.9 Overzicht infrastructuurstandaarden

Type	Info
Aantal datacenters	2
Management	In eigen beheer
Connectiviteit op het netwerk	Eén provider, meerdere Partner-netwerken
Intern netwerk	10 Gbps met gescheiden VLAN-segmenten voor productie en back-up.
Bandbreedte	Internet: 100Mbps (Publilink: 10Mbps Infrax: 4Mbps Telenet: 4Mbps)
Hardware	A-merken met redundante onderdelen en support contract
Storage	Professionele Fiberchannel SAN storage met redundante onderdelen en support contract
Virtualisatieplatform	Vmware met High Availability en Site Recovery (HA+DRS+Geo storage cluster)
Backup	Veeam back-up to disk to disk to tape
Security	Proximus Firewall en Sophos Firewall (beide zonder content checking)
Loadbalancing	Sophos
Ondersteunde besturingssystemen	Windows2008R2 en hoger
Ondersteuning	Op besturingssysteem en Applicatie
Communicatiemogelijkheden	E-mail en telefoon tijdens kantooruren, tijdens uitgebreide kantooruren: via wachtdienst operators (via overname telefoonnummer contactcenter)
Bescherming tegen DDOS aanvallen	In beperkte mate
Monitoring	PRTG
Telesupport	GotoAssist, unattended via Microsoft RD Gateway

3.2 INFORMATIEVEILIGHEID EN GDPR

Cevi en Logins beschikken over een door de Privacycommissie erkende en opgeleide informatieveiligheidsconsulent die deel uitmaakt van een informatieveiligheidscel die ook de directeur ICT en een technisch security officer omvat. De consulent neemt ook de rol van DPO op zich in het kader van de GDPR.

Cevi/Logins beschikt over een door de CEO ondertekend informatieveiligheidsplan.

Cevi/Logins laat zich extern juridisch bijstaan wat GDPR-compliant zijn betreft. Los daarvan werkt Cevi al jarenlang met de nodige vastgelegde interne en externe processen en procedures in verband met personeelszaken, hardwaregebruik, toegangsbeheer gebouwen (zowel voor personeel als voor derden), procedures bij in- en uitdiensttreding, incidenten ... Privacy is trouwens door de aard van de data een inherente taak bij diverse en verschillende medewerkers.

3.2.1 Audits

Het structureel vastleggen van interne audits maakt onderdeel uit van de acties die we, samen met een extern adviesbureau, aan het uitwerken zijn met GDPR comliancy als doel. Dit gebeurt tevens in samenspraak met de NRB-groep (waar Cevi deel van uitmaakt).
In het kader van GDPR compliancy en de verdere uitwerking van ons informatieveiligheidsplan werd een audit gehouden door onze externe juridisch adviseur door middel van een Q&A bij alle afdelingen. Op basis van deze uitkomst en de verdere begeleiding zal nagegaan worden of, hoe en wanneer ook bijkomende externe audits verder noodzakelijk zijn.

Op vlak van financiën en boekhouding gebeuren al externe audits, inclusief naar HRM en interne systemen toe. In het kader van GDPR wordt momenteel nagegaan in hoeverre experten van moedermaatschappij NRB externe audits bij Cevi kunnen uitvoeren.

Er is tevens op regelmatige basis (niet jaarlijks) een audit door het Rijksregister van onze bevolkingstoepassing. Eind 2016 werd er deze audit succesvol uitgevoerd rondom onze WebBV-toepassing (attest daaromtrent ontvangen op 14/12/2016).

Tevens moet Cevi nv jaarlijks een verslag uitbrengen naar Cevi vzw rondom de werking (inclusief inventaris incidenten) van de bevolkingstoepassing. Dit kadert in de erkenning als subregionaal informaticacentrum.

3.2.2 Risicoanalyses

Risicoanalyses worden herzien en geactualiseerd indien noodzakelijk, naar aanleiding van evaluatie van incidenten.

3.2.3 Security & privacy incidentenbeheer

Dergelijke procedures waren voordien in hoofde gekend van de betrokken medewerkers. In het kader van verdere uitwerking van ons informatieveiligheidsplan en GDPR zijn die schriftelijk uitgewerkt.

Cevi gebruikt tal van software/hardware om incidenten te vermijden, op te sporen en te monitoren (zie technische info hierboven).

Bij eventuele incidenten zoals data breach wordt elke situatie apart geëvalueerd door technische specialisten, diensthoofden en directie en wordt er onmiddellijk gereageerd.

Alle incidenten met bijvoorbeeld tijdelijke uitval van toepassingen tot gevolg worden bijgehouden en gedocumenteerd in Sharepoint.

3.2.4 Personeel en opleiding

Alle personeelsleden ondertekenen een arbeidscontract met daarin clausules over privacy en beroepsgeheim.

Elke nieuwe medewerker krijgt, binnen de algemene training van de intern gebruikte tools, ook een training inzake informatieveiligheid. In het kader van de bewustwording en invoering GDPR vonden er in 2018 en 2019 opleidingssessies plaats voor alle werknemers over de inhoud en toepassing van de GDPR. Die opleidingen werden gegeven door een extern advocatenbureau gespecialiseerd in GDPR.

Bij jobkandidaten vragen we een attest van goed gedrag en zeden en volledig CV. Bij aanwervingsgesprekken wordt ingegaan op het beroepsverleden van de kandidaat.

3.2.5 Change management

Er zijn geen generieke, structurele changemanagement procedures aanwezig. Elk project waar er nood is aan change management komt mee op de agenda van het directiecomité en de specifieke implementatie en opvolging van het veranderingstraject wordt daar vastgelegd. Inclusief de verantwoordelijke directeur en projectorganisatie om dit te beheren.

3.2.6 Data eigendom

Cevi is geen eigenaar van de data die het host, maar kan optreden op als verwerker van de data voor zijn klanten. Als een klant zijn contract stopzet, moet de data verwijderd te worden van de systemen bij Cevi.

Waar nodig kan een export van deze data, in de gangbare formaten zoals xml, csv of andere aangeleverd worden de klant.

3.2.7 Toegangen

Toegangen tot zowel de infrastructuur (servers), de databases, de broncode van de toepassingen zijn afgeschermd via authenticatie- en autorisatie mechanismen in Cevi.

Cevi-medewerkers hebben enkel toegang tot deze systemen voor zover dit noodzakelijk is om ze te onderhouden, te monitoren, te diagnosticeren, te upgraden en te beheren. Dit is ook enkel het geval voor de periode dat deze toegang noodzakelijk is.

De credentials van de Cevi-medewerkers die het bedrijf verlaten worden per direct automatisch vernietigd.

Fysieke toegang toe lokalen wordt bepaald via het badgesysteem.

3.3 ISO

Cevi is niet ISO 27xxx gecertificeerd maar verklaart hierbij gelijkaardige maatregelen te hebben genomen op het gebied van kwaliteitsbewaking zoals ook bepaald in de normering rond GDPR en de richtsnoeren van CPBL en KSZ.

4 KWALITEITSCONTROLE EN TESTING

De software ondergaat gedurende en na ontwikkeling een aantal tests om de functionele en technische kwaliteit op niveau te houden.

4.1 TECHNISCHE TESTS

4.1.1 Unit- en Fit-Testen

De software wordt ontwikkeld in Visual Studio. Per functionele module worden er UnitTesten geschreven, die na uitbreiding of aanpassing van de code gelopen worden. Alle tests dienen te resulteren in een positieve assertie, wat garandeert dat de bestaande functionaliteit niet gebroken is.

Verder kunnen voor bepaalde functies ook automatische functionele testen (FIT-testen) gelopen worden (FitNesse https://en.wikipedia.org/wiki/FitNesse).

4.1.2 Automatische code-builds en fouten-notificatie

Om te garanderen dat het gehele softwarepakket ook als technisch geheel functioneel blijft werken, voorzien we automatische build-opdrachten na iedere commit van een afgewerkt stuk software naar ons subversioning-systeem. Hiervoor wordt Jenkins gebruikt.

Bij problemen verstuurt het systeem automatisch notificaties naar de betreffende ontwikkelaars.

4.1.3 Functionele tests

Om functionele testen uit te voeren, voorzien we 3 productomgevingen, met name een development omgeving, een test/acceptatie omgeving en een productieomgeving.

Functionele tests worden uitgevoerd door de ontwikkelaars (development).

De toepassing als geheel wordt door productondersteuners getest in de acceptatie omgeving.

In de productieomgeving is een databank voorzien met fictieve gegevens om de verspreidde productie-versie te testen.

4.2 SOFTWARE VAN DERDE PARTIJEN EN CONTRACTANTEN

Cevi maakt enkel gebruik van eigen geschreven software en componenten van gerenommeerde leveranciers.

De aangekochte componenten worden tijdens de test- en acceptatiefases aan grondige test onderworpen.

Voor de cruciale componenten vraag Cevi ook garanties aan de leveranciers betreffende continuïteit, en vraagt desgevallend ook de broncode ter beschikking te stellen.

4.3 VERSIEBEHEER

Cevi gebruikt in zijn ontwikkelomgevingen Subversion als versiebeheersysteem. Dit garandeert een vlot samenvoegen van code ontwikkeld door verschillende ontwikkelaars. Een ander voordeel van dit systeem is dat, omwille van het backup-regime van de Subversion-server, een automatische garantie dat de broncode van de toepassingen niet verloren kan gaan.
Aansluitend op de acties die op SubVersion gebeuren, kunnen ook automatische builds gelanceerd worden, maar ook automatische deployment naar verschillende testomgevingen.

4.4 TOEPASSINGSBEVEILIGING

De beveiliging van een toepassing wordt duaal aangepakt.

* Authenticatie: toegangsbeveiliging
* Rechten en rollen: functionele beveiliging binnen de toepassing.

4.4.1 Authenticatie

Afhankelijk van de gevoeligheid van de informatie die ontsloten wordt door een toepassing wordt gebruik gemaakt van sterkere of lossere authenticatiemethodes

* Authenticatie op basis van eID of persoonlijk certificaat
  - Voor toepassingen met persoonsgebonden informatie over derden
* Authenticatie op basis van two-factor-authenticatie (Voorbeeld: token van FAS)
  - Voor toepassingen met persoonsgebonden informatie over jezelf.
  - APP, SMS
  - Om deze authenticatie-mogelijkheden te activeren is het gebruik van een eID noodzakelijk.
* Windows-authenticatie
  - Voor toepassingen binnen een gesloten netwerkomgeving (intranet)

Na het leveren van het bewijs van authenticatie wordt er een controle gedaan in ons RBAC-systeem om te verifiëren of er toegang verleend mag worden tot een applicatie.

4.4.2 Rechten en rollen

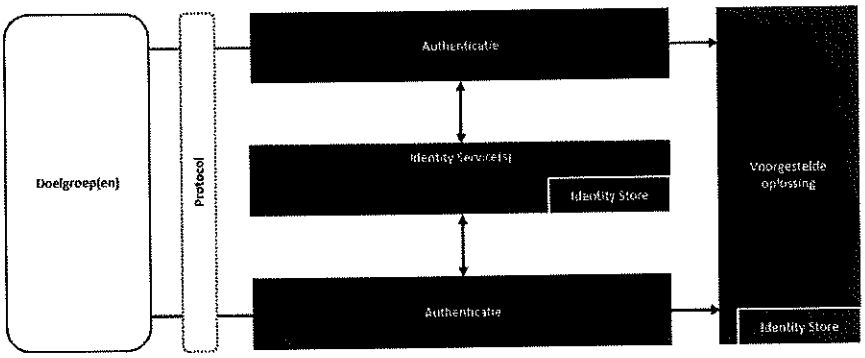
Cevi beschikt over een Role Based Access Control-systeem (RBAC).

Een veiligheidsconsulent kan via een tool (MetaManager) aan gebruikers binnen een bepaalde organisatie een aantal rollen toekennen of afnemen.

Binnen een toepassing kunnen schermen of functionaliteiten afgeschermd worden door ze enkel te ontsluiten voor gebruikers die een bepaalde rol hebben.

Afhankelijk van de rol die je hebt kan ook bepaalde informatie op een scherm afgeschermd of zichtbaar zijn, of heb je al dan niet de mogelijkheid om die informatie aan te passen.

Authentication & autorisation Services



5 LOGGING

Cevi beschikt over logging-systemen waarin verschillende aspecten van het gebruik van de toepassing in opgenomen kunnen worden.

* Aan- en afmelden aan de toepassing
* Registratie van het gebruik, zoals het loggen van een vraagstelling naar private gegevens. Ook het loggen of er een antwoord op die vraag geformuleerd kon worden. Het antwoord op zich wordt niet gelogd, vermits dit zou betekenen dat er private informatie opgeslagen zou worden in de log-databank.
* Wat functionele logging betreft biedt het systeem antwoord op volgende vragen: wie heeft wat opgevraagd, wanneer is dat gebeurd, en was er een antwoord.

Het logging-systeem is onderdeel van het framework waarmee onze toepassingen opgebouwd worden.

6 DATABEVEILIGING

De databanken worden niet rechtstreeks door de toepassingen aangesproken, maar steeds via beveiligde webservices (WCF). De webservices dwingen ook authenticatie af, en de informatie die terugkeert over de webservices is gefilterd op de rechten die je als gebruiker hebt, maar eventueel ook op de informatie die door de opvragende toepassing verwerkt kan worden.
De opvragingen gebeuren steeds over geëncrypteerde lijnen (SSL).

De services zijn ook zo opgebouwd dat code-injectie niet mogelijk is.

De databases worden opgeslagen op dedicated database-servers, waarvan het beheer enkel toegankelijk is door Database administrators.

Wachtwoorden worden versleuteld bewaard, en zijn niet beschikbaar voor toepassingsgebruikers.

Er wordt gewerkt met rollen op de databank. Op deze manier hebben toepassingsgebruikers nooit dbo-rechten, maar enkel de lees- en schrijfrechten nodig binnen het functioneren van de toepassing.

6.1 BEVEILIGINGEN TEGEN OWASP TOP 10 VERSIE 2017

https://www.owasp.org/index.php/Top_10-2017_Top_10

6.1.1 A1 Injection

Toepassingen maken geen gebruik van rechtstreekse verbindingen naar de databank, maar gebruiken hiervoor webservices. Deze webservices lopen steeds over geëncrypteerde verbindingen (SSL), en bevatten geen mogelijkheden om vrije commando's mee te geven. Query's naar de databanken worden via parameters op de server opgebouwd.

6.1.2 A2 Broken Authentication and Session Management.

Toegang tot de data loopt over beveiligde webservices, waarvan de beveiliging gebaseerd is op basis van certificaten.

Op de client dient de gebruiker in bezit te zijn van een certificaat waarvan hij ook de private key heeft. (eID certificaat).

Aan serverside wordt er controle gedaan op geldigheid van het clientcertificaat. Sessies zijn onderhevig aan renegociates.

TLS 1.1/1.2 wordt afgedwongen. SHA1 is onmogelijk gemaakt.

6.1.3 A3 Sensitive Data Exposure

De toepassing geeft geen rechtstreekse toegang tot de data. Deze wordt ontsloten via beveiligde webservices, waarvan de traffic versleuteld is, en er sterke authenticatie via certificaten.
Verder wordt de finaliteit van de data ook gegarandeerd door filters toe te passen op de data en de functionaliteit op basis van een RBAC-systeem, waar aan een gebruiker rollen

moeten worden toegekend, die hem/haar al dan niet recht geeft om de data of functionaliteit te kunnen gebruiken.

6.1.4 A4 Xml External Entities

Entiteiten worden via WCF binair opgenomen via clientconnectoren die Cevi zelf voorziet. Daardoor is het publiceren van bijvoorbeeld Metadata exchange informatie op productie-eindpunten van webservices niet nodig (MEX).

Cevi beschikt in zijn datacenter ook over gescheiden interne en externe netwerken. Verwijzingen naar interne resources, mochten die er als zijn, resulteren hierdoor in broken links waardoor deze interne resources niet exposed worden.

6.1.5 A5 Broken Access Control

De toepassingen maken gebruik van een RBAC-systeem, waarbij bij elke functie-oproep controle wordt gedaan op de noodzakelijke rechten van de gebruiker.

Als de sessie over de beveiligde services verbroken is, kan zal deze controle geen positieve assertie kunnen teruggeven en dus ook geen toegang tot de data of functionaliteit.

De toepassing heeft geen rechtstreekse toegang tot de database.

6.1.6 A6 Security Misconfiguration

Configuratie van de toepassing en services worden opgebouwd van een lege situatie, waardoor defaults niet aanwezig zijn. Omwille van het click-once deployment systeem garanderen we dat de toepassingen steeds up-to-date zijn.

Serverside zijn de services bij Cevi gehost, en onderhevig aan de nodige automatische updates van het besturingssystemen.

6.1.7 A7 Cross Site Scripting

In zijn webtoepassingen vermijdt Cevi het gebruik van Cross-site scripts.

6.1.8 A8 Insecure deserialization.

Onbeveiligde deserialisatie wordt tegengegaan door op netwerkniveau beveiliging toe te passen. In hoofdzaak gaat dit over het toepassen van messagesecurity waarbij gevoelige data ondertekend wordt met certificaten. Data wordt ook referentieel en inhoudigelik gevalideerd.

6.1.9 A9 Using components with known vulnerabilities

Bij het ontwikkelen van de software worden enkel eigen componenten als componenten van gerenomeerde bedrijven gebruikt. Bij ontwikkeling maken we daarbij gebruik van hun officiële deployment packages. Via NuGet worden die ook automatisch beschikbaar gesteld, en op deze manier in de toepassing opgenomen.
Click-once zorgt ervoor dat het deployment naar de klant rap doorgevoerd wordt.

6.1.10 A10 Insufficient Logging&Monitoring

Cevi beschikt over logging-systemen waarin verschillende aspecten van het gebruik van de toepassing in opgenomen kunnen worden.

* Aan- en afmelden aan de toepassing
* Registratie van het gebruik, zoals het loggen van een vraagstelling naar private gegevens. Ook het loggen of er een antwoord op die vraag geformuleerd kon worden. Het antwoord op zich wordt niet gelogd, vermits dit zou betekenen dat er private informatie opgeslagen zou worden in de log-databank.
* Wat functionele logging betreft biedt het systeem antwoord op volgende vragen: wie heeft wat opgevraagd, wanneer is dat gebeurd, en was er een antwoord.

Het logging-systeem is onderdeel van het framework waarmee onze toepassingen opgebouwd worden. Lokaal verzamelde log-acties kunnen naar een centraal logsysteem geconsolideerd worden om forensisch onderzoek te doen over verschillende toepassingen heen.

Daarnaast is er ook een technische monitoring van de services mogelijk, waarbij onverwachte pieken in geheugen, netwerk traffiek of processorgebruik tot alarmsignalen kunnen escaleren. (**Application Domain Resource Monitoring**)