Security & Privacy

Beveiliging van persoonsgegevens en bedrijfsgevoelige informatie kan rekenen op ruime aandacht van overheden en leveranciers. Het grote aantal meldingen van datalekken, de forse toename van slachtoffers van identiteitsfraude, de voortdurende dreiging van cyberaanvallen en de geslaagde gijzelingen met ransomware laten zien dat die aandacht nog steeds terecht is.

Als leverancier van softwareproducten en diensten en als verwerker heeft Centric in de afgelopen jaren maatregelen getroffen voor de beveiliging van gevoelige gegevens. Met deze maatregelen ondersteunen wij onze klanten om te kunnen voldoen aan de eisen die gesteld worden in wet- en regelgeving, zoals de Algemene verordening gegevensbescherming (AVG), het normenkader ICT-beveiligingsassessment DigiD, de Baseline Informatiebeveiliging Overheid (BIO) en de Eenduidige Normatiek Single Information Audit (ENSIA). Dit vanzelfsprekend in combinatie met de maatregelen die binnen de klantorganisatie moeten worden getroffen.
Nieuwe wet- en regelgeving, zoals de NIS2-richtlijn, en ook nieuwe bedreigingen vereisen steeds weer aanvullende beveiligingsmaatregelen.

De BIO 2.0 met bijbehorende handreikingen en thema-uitwerkingen is een voorbeeld van vernieuwde regelgeving. Het beveiligen van onze softwarediensten is daarom geen eenmalige actie, maar een belangrijk onderdeel van ontwikkeling, dienstverlening en beheer, in een continu proces. Omdat Centric steeds meer als cloud serviceprovider opereert, mogen onze klanten verwachten dat we ook proactief onze verantwoordelijkheid nemen om de data van klanten in onze omgeving te beveiligen.
Hierna staat beschreven hoe Centric invulling geeft aan het beleid voor informatiebeveiliging. Met de maatregelen die genomen zijn of worden om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen voor onze producten en diensten, en hoe Centric klanten helpt tegen de eerdergenoemde dreigingen. Meer informatie over hoe Centric omgaat met de thema's security en privacy vind je in ons Centric Trust Center. Ook verwijzen wij u graag naar de recent verschenen Whitepaper SaaS en security. Een toelichting op de producten die Centric biedt op het gebied van security en privacy vind je in de hoofdstukken over onze afzonderlijke producten.

Security

Centric beleid informatiebeveiliging

Centric heeft een informatiebeveiligingsbeleid opgesteld waarin de uitgangspunten en stuurmechanismen benoemd zijn voor een veilige verwerking van gegevens. Het beleid is uitgewerkt in concrete procedures en maatregelen en is van toepassing voor alle Centric-medewerkers.

Secure Software Development

De basis voor security ligt bij de ontwikkeling van veilige software. Centric gebruikt hiervoor de methode en normenkaders van Secure Software Development (SSD) van het Centrum Informatiebeveiliging en Privacybescherming (CIP). Wij passen daarbij de methode Grip op SSD toe, hierdoor hebben klanten inzicht in onze werkwijze voor het ontwikkelen van veilige software. Centric heeft actief bijgedragen aan vernieuwing van de SSD-normen, versie 3. De security requirements van SSD zijn opgenomen in de Centric Baseline voor secure software development en zijn voorwaarde bij de (door)ontwikkeling van onze software.
Om het veilig ontwikkelen van software nog meer handen en voeten te geven, heeft Centric begin 2022 de 'Shift Left'-beweging ingezet. Dit houdt in dat securityvereisten vanaf het eerste stadium in het softwareontwikkelproces worden meegenomen en in elke opvolgende fase opnieuw aandacht krijgen.

Structurele toetsing

Centric heeft een eigen team van ethische hackers (het Red Team) dat structureel - pentesten uitvoert op onze softwareproducten en -diensten. Bij het testen wordt onder andere gebruikgemaakt van de SSD-normenkaders, de Top 10 Application Security Risks van Open Web Application Security Project (OWASP), de Nationaal Cyber Security Centrum (NCSC) ICT-Beveiligingsrichtlijnen voor webapplicaties en mobiele applicaties en andere CVE's (Common Vulnerabilities and Exposures). De bevindingen van deze pentests leiden tot aanpassingen binnen onze software. Voor het classificeren en prioriteren op basis van de (technische) ernst van de gevonden kwetsbaarheden wordt CVSS 3.1 aangehouden. CVSS staat voor Common Vulnerability Scoring System en ook dit is een open industriestandaard. Op basis van de aldus bepaalde risico's en prioriteiten worden de kwetsbaarheden verholpen.
Naast deze periodieke toetsing van onze producten vindt er ook continue toetsing van onze producten plaats met zogenaamde Application Security Testing (AST) tools. Deze tools worden gebruikt om de kwaliteit en veiligheid van software in kaart te brengen en op onderdelen zelfs af te dwingen. Voorbeelden hiervan zijn SonarQube, Sigrid, Dependency Check en Netsparker. Naast het meten van de kwaliteit van de code, worden hierdoor ook security analyses uitgevoerd en vinden er geautomatiseerde controles plaats op bekende kwetsbaarheden. Dit omvat de code die we zelf ontwikkelen. En ook de gebruikte open source software en componenten van derden, de zogenaamde software supply chain, worden meegenomen in de analyses en controles.

Monitoring kwetsbaarheden en dreigingen

Centric beschikt over een eigen Security Operations Center (SOC) dat verantwoordelijk is voor threat detection & response. Dit team van securityspecialisten monitort het Centric-netwerk met behulp van verschillende tools. Eén van deze tools is Microsoft Sentinel, een Security Incident en Event Management (SIEM) tool, die intelligente beveiligingsanalyses en dreigingsinformatie biedt. Deze tool combineert data die wordt gegenereerd uit verschillende beveiligingscomponenten, zoals Microsoft Defender, logregels van servers, DDoS-bescherming en firewalls om een zo compleet mogelijk overzicht te bieden voor onze securityspecialisten. Deze securityspecialisten zijn een belangrijke schakel in onze beveiligingsketen.

Als er al iets voorbij de opgeworpen barrières zou komen, dan is het hun taak dit zo snel mogelijk te signaleren en passende maatregelen te treffen. Aanvullend biedt Centric klanten een threat detection & response dienst aan.

DigiD-assessments

Logius vereist een jaarlijks ICT-beveiligings-assessment voor applicaties die DigiD gebruiken. Voor dit assessment heeft Logius een normenkader opgesteld. De toetsing moet worden uitgevoerd door een Register EDP-auditor. Voor de betreffende applicaties laat Centric jaarlijks een externe auditor een assessment uitvoeren voor het applicatiegedeelte en het hostingsgedeelte. De Third Party Memorandum (TPM) die we aan onze klanten ter beschikking stellen dekt hiervoor relevante normen af. Ons streven is deze TPM uiterlijk medio oktober aan onze klanten te leveren. Elke klant moet daarnaast een audit op het eigen securitybeleid laten uitvoeren. Onze TPM kan samen met het gedeelte van de klant bij Logius ter verificatie worden aangeboden.

ISO 27001

Centric heeft voor de levering van (cloud)diensten een informatiebeveiligingsmanagementsysteem (ISMS) opgesteld en geïmplementeerd conform de beveiligingsnorm ISO 27001. De beheeractiviteiten die worden uitgevoerd voor clouddiensten zijn volgens deze norm gecertificeerd. Op basis van jaarlijkse risicobeoordelingen, audits, wijzigingen in wet- en regelgeving en business requirements scherpen we ons informatiebeveiligingsbeleid continu aan. In 2021 is de ISO 27001-certificering voor het software ontwikkelproces behaald. Daarmee voldoen we aantoonbaar aan de eisen die markt en toezichthouders stellen. Voor 2024 geldt dat we zullen overgaan op de nieuwste versie van de ISO 27001-standaard, namelijk de 2022-versie.

Privacy

Na het van kracht worden van de AVG in mei 2018 is meer duidelijkheid gekomen over de interpretatie en invulling van deze privacywet. Centric heeft in samenwerking met de Privacy Company een Centric Baseline Product Privacy opgesteld. Hierbij is gebruikgemaakt van het Privacy by Design Framework van de Privacy Company. Deze baseline is gebruikt om de bestaande applicaties te toetsen aan de AVG. Naar aanleiding van bevindingen hieruit zijn aanpassingen doorgevoerd. Ook bij nieuwe ontwikkelingen stellen we met behulp van deze baseline de privacy-eisen vast. Ook heeft Centric bijgedragen aan de totstandkoming van de Privacy by Design-instrumenten die de Informatiebeveiligingsdienst (IBD) beschikbaar heeft gesteld.

De AVG stelt rechtmatigheid, behoorlijkheid en transparantie bij de verwerking van persoonsgegevens voorop. Gegevens mogen uitsluitend worden verwerkt in het kader van een gerechtvaardigd doel en dan ook alleen die gegevens die echt noodzakelijk zijn. Ook mogen gegevens niet langer bewaard blijven dan noodzakelijk. Tevens hebben rechthebbenden het recht om te weten welke gegevens er van hem/haar bekend zijn en welke verwerkingen er hebben plaatsgevonden. Hierbij biedt Centric Privacy Workspace ondersteuning.

Verwerkersovereenkomst

De AVG schrijft voor dat bij verwerking van persoonsgegevens door een verwerker (in dit geval Centric) de afspraken en maatregelen om een veilige verwerking te garanderen worden vastgelegd in een verwerkersovereenkomst. De verwerkersovereenkomst maakt deel uit van het contract.
Centric heeft meegewerkt aan de standaard verwerkersovereenkomst van de Vereniging van Nederlandse Gemeenten (VNG) en gebruikt de meeste recente versie (augustus 2023). Daarnaast heeft Centric meegeholpen aan het opstellen van een factsheet om te bepalen in welke gevallen een leverancier een verwerker is (in de zin van de AVG) en dat daarom een verwerkersovereenkomst moet worden afgesloten.

Privacy statement

Centric heeft een privacyverklaring opgesteld, Centric heeft een privacyverklaring opgesteld, deze is op onze site te vinden. Naast algemene zaken is hier informatie te vinden over specifieke verwerkingen die Centric voor haar klanten uitvoert in het kader van support en conversies.

ISO 27701

Centric is voornemens om in 2024 het Privacy Information Management System (PIMS) te laten certificeren op de internationale privacy standaard ISO 27701. Deze standaard is een aanvulling op de informatiebeveiligingsnorm ISO 27001 en richt zich op het beheer van persoonlijke informatie en de risico's die daarbij komen kijken. Bovendien helpt het bij het aantonen van de naleving van privacywetgeving, zoals de Algemene Verordening Gegevensbescherming.