

## Centrum voor Publieke Innovatie waarborgt veiligheid van gevoelige persoonsinformatie met security testing Computest



centrum  
voor publieke  
innovatie

**Centrum voor Publieke Innovatie (CPI)** brengt vernieuwende maatschappelijke ideeën vanuit gemeenten of publieke organisaties in de praktijk door ondersteuning te bieden met innovatieve concepten of techniek. Veiligheid is vanzelfsprekend een belangrijk aandachtspunt bij projecten met gemeenten en voor applicaties waarbij met gevoelige persoonsinformatie wordt gewerkt. Het CPI schakelde daarom Computest in voor het testen van de security van diverse applicaties.

CPI is een snelgroeiende en veelzijdige organisatie met ruim 20 medewerkers. Het ontwikkelde onder meer applicaties voor gemeenten en professionele (jeugd)zorgverleners, maar ondersteunde ook bij de bouw van een hotelclassificatiesysteem.

### Aanleiding security testing

Roberto Bosco, productmanager bij CPI, is verantwoordelijk voor productontwikkeling en -realisatie en de gebruikerservaring: "Directe aanleiding voor het inschakelen van hulp bij security testing is de markt waarin we opereren: we hebben onder andere te maken met gemeenten, jeugd- en volwassenenzorg. Dat betekent dat er gevoelige informatie in onze applicaties opgeslagen is."

De applicatie **MULTisignaal** bijvoorbeeld, is een hulpmiddel voor gemeenten en zorgverleners. In deze applicatie worden alle instanties/professionals die betrokken zijn bij de zorg voor een cliënt (jeugdige) met elkaar in contact gebracht. Zo krijgen ze een volledig beeld rondom de jeugdige en kunnen ze tot één plan komen. Veiligheid is van groot maatschappelijk belang voor deze applicatie.

"We hebben te maken met gemeenten, jeugd- en volwassenenzorg. Dat betekent dat er gevoelige informatie in onze applicaties opgeslagen is."

Roberto Bosco, productmanager bij CPI

Dat geldt ook voor de applicaties Veilig Thuis Register (een adviespunt en meldpunt kindermishandeling en huiselijk geweld) en Meldpunt Fraude in de Zorg (meldpunt voor vermoeden van zorgfraude).

"We houden ons al jaren bezig met security testing en werkten hiervoor al samen met een externe partij. We misten bij die partij echter de verbondenheid met onze organisatie, het begrip van wat we doen. Daarom besloten we een andere partner te zoeken", aldus Bosco. "We benaderden een aantal partijen, hebben ze allemaal gesproken en legden twee van hen nog extra vuur aan de schenen met een assessment. Met Computest hadden we gelijk

een klik. Ze vragen door, snappen de bredere context én gaan de dialoog aan. We hebben nu het gevoel dat we samenwerken met een partner die begrip heeft voor wat wij, als CPI, aan het doen zijn en wat voor ons van belang is.”

### Vulnerability testing

De **security testers** van Computest kregen de opdracht om de meest belangrijke functionaliteiten op security-vlak, zoals de implementatie van de authenticatie, API-functionaliteit en een push bericht-functionaliteit, te controleren. Ze onderzochten de applicaties Veilig Thuis Register en MULTIsignaal.

“Omdat onze applicaties aan verandering onderhevig zijn laten we deze met regelmaat testen. Bijvoorbeeld na een wetswijziging zoals de invoering van de AVG. Soms geven we een specifieke invalshoek voor de focus van een test aan, bijvoorbeeld als we een nieuwe API gerealiseerd hebben. Computest denkt echter wel mee in het opstellen van de scope. Zij hebben immers de laatste kennis op het gebied van nieuwe kwetsbaarheden.”

Computest voerde een uitputtend vulnerability onderzoek uit. Hierbij werd gebruik gemaakt van de **gerenommeerde Certified Secure checklist**. Deze omvat onder andere de **OWASP-top 10** en **NCSC-richtlijnen**. Op basis van deze verschillende pentesten worden alle mogelijke kwetsbaarheden nagelopen. Per item resulteert dit in een score van 1 tot 10.

### Dialoog

Bosco: “Er zijn altijd bevindingen na zo’n test, juist in situaties waarin continu zaken veranderen. We zijn dus erg blij met de feedback. Onze primaire zorg voor veiligheid is iets wat niet verandert.

Wij leggen onszelf het ‘pas toe of leg uit’-principe op, wat betekent dat we aanpassingen doorvoeren óf moeten verantwoorden waarom we dat niet doen. Ook hierin is Computest een goede partner gebleken: tijdens de initiële terugkoppeling ontstond er een levendige dialoog tussen onze technisch architecten, de producteigenaren en de testers over het wel of niet doorvoeren van aanpassingen.”

### Menselijke testers

Bosco waardeert ook de betrouwbaarheid en sterke focus van Computest: “Het is geen automatisme, geen ‘gooi er een muntje in en er rolt iets uit’. Er zijn menselijke testers aan het werk, ze stellen vragen, er wordt menselijke intelligentie toegevoegd. Dat is een grote meerwaarde. Onze applicaties zijn maatwerk en te complex om er een geautomatiseerde test op los te laten.”

### Third party memo

Computest stelde na de security testen een zogenaamde Third Party Memo (TPM) op. Hierin staat beschreven wat er getest is en wat de status daarvan is. Dit afschrift van een security-rapport kan gedeeld worden met belanghebbenden om de veiligheid van applicaties aan te tonen, bijvoorbeeld voor een samenwerking met gemeenten.

“Zo’n rapport is een leerzaam traject. Bovendien worden onze andere applicaties indirect ook sterker: als er een kwetsbaarheid wordt gevonden in een applicatie, onderzoeken we direct of dit voor andere projecten ook geldt”, aldus Bosco. “Dit sluit goed aan bij onze filosofie. Het CPI hanteert het principe dat alles wat met publiek geld betaald wordt, maar één keer betaald hoeft te worden. We ‘hergebruiken’ beproefde strategieën en vertalen deze van sector a naar sector b. Dat is onze kracht.”



**Computest**  
always on.

info@computest.nl  
+31(0)88 733 13 37  
www.computest.nl

We zijn een team van gepassioneerde en ervaren technisch specialisten die applicaties en infra-structuren optimaal laten werken. Wij geloven in geïntegreerde quality assurance en bieden daarom diensten op het gebied van performance, security en functionele testautomatisering.

In alles wat we doen worden we gedreven door een grenzeloze passie voor kwaliteit. Daarom werken we voor iedere sector samen in kleine, gespecialiseerde agile teams. Daarmee houden we de lijnen kort zodat we de beste resultaten behalen.