



TECHNISCHE SWOT

Wanneer een product of een dienst gelanceerd wordt, geeft een **S W O T**-analyse ('Strenghts' (sterktes), 'Weaknesses' (zwaktes), 'Opportunities' (kansen), 'Threats' (bedreigingen)) aan op welke sterktes en kansen kan worden voortgebouwd, maar ook met welke bedreigingen en zwaktes rekening moet worden gehouden.

In ons geval stelt deze analyse ons in staat om de drie systemen te vergelijken en vanuit een breder perspectief te analyseren.





Sterktes

- Beveiligde infrastructuur (private cloud)
- Datacenters die voldoen aan normen: ISA 3402 type 2, ISO 9001, ISO 270001, enz.
- Veerkracht in geval van een ramp
- Bekend en snel authenticatieproces (CSAM)
- Mogelijkheid om voor elke oplossing de juiste technologie te gebruiken dankzij de microservices-architectuur
- Flexibiliteit van de infrastructuur om de middelen en kosten van elke dienst te optimaliseren in functie van de behoeften
- Traceerbaarheid van de acties voor audits
- Futureproof architectuur (containers as a service, CaaS)
- Stateless softwarearchitectuur (schaalbaarheid)
- Beveiligingsmechanismen op "ondernemingsniveau" die een hoge mate van betrouwbaarheid garanderen in vergelijking met papieren stembussen
- Het systeem is blootgesteld via virtuele privénetwerken (VPN), wat de bedreigingen van buitenaf beperkt.

Kansen

- Innovatie & technologische vooruitgang
- Combinatie & integratie van huidige systemen
- Mogelijkheid om geavanceerde functionaliteiten te implementeren zoals real-time monitoring van de opkomst, enz.
- Samenwerking met onderzoeksinstituten om de veiligheid van het systeem continu te verbeteren
- Potentiële uitbreiding van het e-votingsysteem naar andere domeinen, zoals verkiezingen voor particuliere organisaties
- “State of the art” technologie, conferenties en belangstelling van de IT-gemeenschap

Zwaktes

- Hosting- en onderhoudskosten (private cloud) Moeilijke
- integratie met andere tools
- Complexiteit & ontwikkelingskosten
- Hoge SLA, met een lage verhouding tussen toegevoegde waarde en kosten Mogelijkheid van technische storingen, wat leidt tot potentiële problemen tijdens verkiezingen
- Moeilijkheid om van een 'private cloud'-platform naar een ander te migreren
- Het stemgeheim kan alleen worden gegarandeerd door een sterke governance: niemand heeft gelijktijdig toegang tot de informatie die een gebruiker en een stem met elkaar verbindt.
- Beheer van een vloot stemcomputers (kiosken), waarvoor de verantwoordelijkheid gedeeltelijk is overgedragen aan de gemeenten.

Bedreigingen

Blootstelling aan het internet (veiligheidsrisico's)

- Geen standaard regelgeving
- (lokaal, nationaal en Europees), potentiële impact in de toekomst
- Behoeft aan geavanceerde technologische competenties om het platform te ontwikkelen en te onderhouden
- Mogelijkheid van bugs of onopgemerkte kwetsbaarheden in het systeem die kunnen worden uitgebuit door kwaadwillenden Risico van hacken of
- manipulatie van verkiezingsresultaten
- Gevoelig voor storingen in de stemcomputers (kiosken).
- Ongecontroleerde veroudering van stemcomputers.
- De kwaliteit van het gemeentelijke netwerk kan niet worden gegarandeerd