



SUCCESS STORY

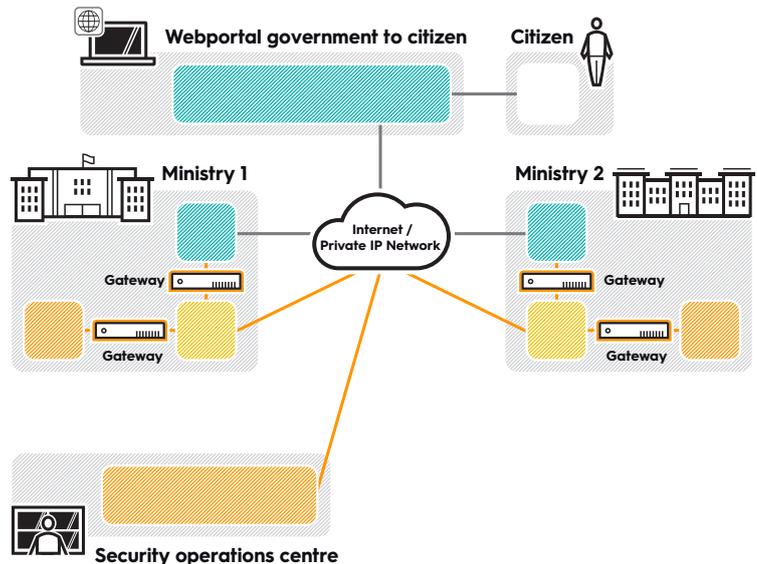
Informationssicherheits- konzept für sicheres e-Government

Regierungs- und Behördenorganisationen setzen zur Erfüllung ihrer Aufgaben zunehmend neue Informations- und Kommunikationstechnologien ein, um die Effizienz und Transparenz zu erhöhen.

Da im Rahmen von e-Government grosse Mengen an sensiblen Informationen bearbeitet, häufig über mehrere Ministerien hinweg ausgetauscht und zentral in Datenzentren gespeichert werden, ist der Sicherheitsaspekt bei der Planung und Implementation von e-Government-Projekten von zentraler Bedeutung.

Sicheres e-Government

- Entsprechend der Klassifizierungsstufen der Informationen geschützte Kommunikationsverbindungen: einerseits interministerial, andererseits zwischen Ministerien und Bürger
- Informationen werden je nach ihrer Klassifizierung in unterschiedlichen Sicherheitszonen bearbeitet und gespeichert.
- Die verschiedenen Sicherheitszonen können Trusted-, Secure- oder High-Security-Zones sein, wobei in jeder Zone auch tiefer klassifizierte Informationen bearbeitet werden können
- Anbindung eines Security Operation Centres (SOC) zur Überwachung der Infrastruktur
- Performante Netzwerklösungen sowie End-zu-End-Chiffrierlösungen der CyOne Security zum Schutz der interministerialen Kommunikationsverbindungen
- Schutz der Perimeter und Zonenübergänge



Projektspezifikation

- Massgeschneidertes e-Government-Informationssicherheitskonzept für den bestehenden Netzwerkbackbone
- Definition und Implementation von Sicherheitszonen entsprechend den bestehenden Klassifizierungsstufen
- Angemessener Schutz der Perimeter und Zonenübergänge
- Zentrale Verwaltung und Überwachung der Infrastruktur

Implementation

- Planung und Implementation eines ganzheitlichen, kundenspezifischen e-Government-Informationssicherheitskonzepts, welches die bestehenden Klassifizierungsstufen der schützenswerten Informationen berücksichtigt
- Projektabwicklung und Lieferung aus einer Hand, vom Konzept bis zur Infrastruktur
- Kundenspezifisch konzipierte, leistungsfähige Netzwerk- und End-zu-End-Chiffrierlösung für den hochsicheren Austausch von klassifizierten Informationen
- Perfekte Integration der Chiffrierlösung in die bestehende Infrastruktur
- Schutz der Perimeter und Zonenübergänge durch Security Gateways
- Aufbau eines zentralen Security Operation Centres (SOC) zur Überwachung der Infrastruktur
- Umfassender Wissenstransfer an die lokalen Systemverantwortlichen

Höchste Sicherheit

Die einzigartige Sicherheitsarchitektur der CyOne Security bietet bestmöglichen Schutz der sensiblen Informationen vor unerwünschtem Abhören – zudem können diese aufgrund des kundenspezifischen Benutzer- und Berechtigungsmanagements ausschließlich von authentifizierten Benutzern eingesehen und bearbeitet werden.

Perfekte Integration

Der Security-Layer lässt sich perfekt und kostensparend in die bestehende Infrastruktur integrieren – inklusive SOC.

Hohe Verfügbarkeit

Redundant implementierte Kommunikationskanäle gewährleisten die ständige Verfügbarkeit und Ausfallsicherheit.

Unabhängiger Betrieb

Das gesamte, hoch performante Netzwerk kann durch die Systemverantwortlichen infolge umfassenden Wissenstransfers autonom betrieben werden.