Naam van de G-Clouddienst

Internet Access Protection / Security as a Service ***01-01-2020***

Omschrijving van de G-Clouddienst

G-Cloud biedt overheidsinstellingen IT-beveiligingsdiensten aan via twee verschillende mogelijkheden die toepasbaar zijn naargelang de context van de instelling. Technisch gezien zijn beide diensten heel gelijklopend, de grootste verschillen situeren zich in de governance en de contractvorm.

1. Internet Access Protection

Modulair aanbod van beveiligings-infrastructuurcomponenten gebaseerd op een combinatie van infrastructuurlastenboeken, dienstverlening en dienstencontracten geleverd door Smals.

Er zijn verschillende beheersmogelijkheden waarbij klanten zowel een fully managed service kunnen afnemen als zelf beheerde veiligheidsinfrastructuur. IAP wordt binnen de overheidscommunity beheerd met sterke focus op de business en datacenter behoeften.

Het platform is geïnstalleerd in de G-Cloud datacenters (IN en UP) met uitzondering van een externe SIEM dienst (Proximus).

2. Security as a Service

Security as a Service is een Risico management Service, het omvat een pakket van Security en Governance diensten met een onderliggende infrastructuur, zoals een risicoregister en het opvolgen van gedetecteerde potentiële risico's.

Deze dienst is een fully managed service, na een overheidsopdracht gegund aan Proximus, voor beveiliging van infrastructuur-componenten. Dit contract bevat een eveneens een sterke bureautica-beschermingscomponent en steunt op een grote userbasis van FOD Financiën en FOD Justitie als start.

Het platform is geïnstalleerd in de G-Cloud datacenters (Noga en Finto), met uitzondering van de management-platformen van Proximus en een aantal externe diensten voor DNS/Mail security/DDoS en SIEM.

Naam van de G-Clouddienst

Internet Access Protection ***01-01-2020***

Omschrijving van de G-Clouddienst

Met IAP wordt een centraal platform ter beschikking gesteld van de federale instellingen om de toegang naar en van het Internet te beveiligen. Dit platform heet Internet Access Protection (IAP) en is gebaseerd op het Extranet-beveiligingsconcept ontworpen door Smals.
Via IAP kunnen de federale instellingen rechtstreeks en op een beveiligde manier met elkaar communiceren en informatie uitwisselen zonder langs Internet te moeten passeren.
Smals biedt verschillende beheersmogelijkheden waarbij klanten zowel een managed service kunnen afnemen als zelf beheerde veiligheidsinfrastructuur. De dienst is modulair opgebouwd, volgens de behoeften van de klant, om de controle te behouden over de beveiliging en de bijbehorende business.

IAP kan beschouwd worden als het gemeenschappelijke “schild” in de informatiebeveiliging, en omvat de volgende diensten:

- IAP basispakket:
  - Verbinding naar Internet via FedMAN, beveiligd met :
    - Firewalling
    - IDP (Intrusion Detection Prevention)
    - Anti-DDoS
    - SIEM (Security information and event management operations)
  - DNS (Domain Name System) met replicatie naar ‘external’ DNS systeem
  - NTP (Network Time Protocol) service (Stratum 1)
- IAP opties:
  - Proxy User en antivirus (incl. sandboxing) voor beveiliging van http(s) en (s)ftp-verkeer
    - Web-filtering / Web reputation
    - Sandboxing (Advanced Threat Protection)
    - SSL-Inspection
  - Mail routering met Antispam en Antivirus (incl. sandboxing)
    - Antispam / Antipishing en quarantaine management delegation
    - Twee lagen Internal / external mails routering
    - Sandboxing (Advanced Threat Protection)
  - VPN (Virtual Private Network) voor toegang vanop afstand met with advanced identity management en compliancy check
- Bijkomende diensten:
  - Site-to-site VPN
  - Application Delivery Control (ADC) met SSL offload en web-app security
  - Connectivity en IP compliancy management (NAT). Elke instelling kan bijkomende maatregelen nemen om de systemen met IAP te verbinden en intern te beveiligen. De veiligheids- en netwerkspecialisten van G-Cloud kunnen u hierbij in raad en daad bijstaan.

Service owner

KSZ – Jean Jochmans – iap@gcloud.belgium.be

Service level agreements

- Beschikbaarheid: 99,9%
- Performantie: verbinding met Internet <10ms
- Service window: 24/7
- Support window: 24/7
- Support 1ste/2de lijn: G-Cloud Frontoffice (frontoffice@gcloud.belgium.be)
- Support 3de lijn: Network Infra Team en andere teams
- Setup: 2 werkweken

Kostprijsregeling

De kosten worden volgens het pay per use principe aangerekend.

Wat is de voorziene verdere evolutie van de dienst ?

De gevaren van het internet evolueren voortdurend. De dienst IAP dient hierop soepel te reageren door continu naar verbetering te streven.
Technical user Boards houden regelmatig plaats en laten de leden toe hun ervaring en hun behoeften uit te wisselen, alsmede technische evolutie te bespreken.

Praktische info

Meer info via **iap@gcloud.belgium.be**

Naam van de G-Clouddienst

Security as a Service ***01-01-2020***

Omschrijving van de G-Clouddienst

G-Cloud *Security as a Service* omvat zowel bescherming van Internet als bescherming van interne endpoints via flow-based en host-based security. Deze dienst beveiligt het verkeer op alle netwerkniveau's, van LAN tot Internet.

De dienst omvat het materiaal, licenties, opzet, migratie, onderhoud, governance, CSOC assistentie, audit, training, vulnerability assessment, pentesting, technology survey.
Aan de hand van deze services wordt de informatie tussen gebruikers en servers via LAN, Wireless LAN, private WAN, publiek internet en publiek mobiel netwerk beveiligd.
Security as a Service is een Risico management Service, het omvat een pakket van Security Governance diensten met een onderliggende infrastructuur, zoals een risicoregister en het opvolgen van gedetecteerde potentiële risico's.

Security as a Service kan beschouwd worden als een gedeelde infrastructuur voor federale overheidsdiensten voor zowel het voorkomen en detecteren van veiligheidsincidenten als het reageren en anticiperen erop. Beide aspecten zijn dus inbegrepen, state of the art preventie en snelle reactie in geval van een incident.

Deze dienst is gebaseerd op Security dienstverlening van Proximus in het kader van een lastenboek van FOD Financiën.

De beveiligingsinfrastructuur is geïnstalleerd in de G-Cloud datacenters in gebruik door FOD Financiën met uitzondering van de managementplatformen van Proximus en een aantal externe diensten voor DNS/Mail security/DDoS en SIEM.

Het basispakket omvat volgende elementen:

- Installatie en assistentie bij het opstarten
- Migratie van de bestaande infrastructuur
- Opzetten van het Security Operation Center (SOC)
- Aansluiting van de interne en externe netwerken en de servers op de DMZ
- Externe beveiliging
    - Dubbele redundante firewall-laag
    - Bepaling en beveiliging van de DMZ's
    - Priorisering van de gegevensstromen
    - Priorisering van bepaalde URL's
    - Ondersteuning van de fysieke en virtuele netwerken
    - Integriteit van het webverkeer
    - Begrenzing van ongewenste websites
    - Site-to-site VPN
    - Intrusion Detection and Prevention
    - Host based Security
    - Integriteit van het e-mailverkeer
    - Antispam en antiphishing
    - Beveiligd DNS-systeem

  - Controle on demand op malware in bestanden
  - Web Application Firewall
  - Sandboxing
  - Advanced Malware protection
  - Advanced Threat protection
  - Distributed Denial Of Service (DDOS) protection – Application based
  - Application control
  - Botware protection
  - Data leakage protection
  - Antivirus protection
  - Compliancy check
  - SSL inspection
  - Surf protection & control
  - Identity awareness
- Interne beveiliging
  - Load balancing + Web App Protection
  - Secure messaging with malware / ransomware protection
  - Managed Security Services and Security Operations Center (SOC)

Beschikbare extra opties zijn:

- Remote Access voor medewerkers, IT-beheerders en partners
  Met ondersteuning van de Belgische eID-identiteitskaarten, CAC-kaarten (Common access card), elektronische tokens en OTP (One-time password)
- End point Software Security Agent
- Mobile Device Protection (VPN)
- Remote SSL server
- Network Access Control (NAC)
- IP address management, DNS, DHCP
- Advanced security for end-points
- Security Information and Event Management (SIEM): Interne netwerkbewaking
- DDOS protection and volume based attacks protection
- CSIRT-services (Computer Security Incident Response Team)
- Services Security & GDPR compliancy
  - Vulnerability Management
  - Vulnerability Automatic Assessment & VAM
  - Asset & Lifecycle management
  - Cyber threat feeds
  - Service quality survey & management
  - Technology survey & best practice recommandations
  - Security Awareness
  - Management report
  - Regular Pentesting & compliance audit

Service owner

FOD Financiën - Frank Van De Heijning - secaas@gcloud.belgium.be

Service level agreements

- Beschikbaarheid: 99,9%
- Performantie: verbinding met Internet <50ms
- Service window: 24/7
- Incident response time: binnen 1 uur voor Priority 1
- Incident resolution time: 2 uur
- Boeteclausule: max. 6,5 % van de fee op basis van de maandelijkse beschikbaarheidscijfers
- Support 1ste/2de lijn: Proximus
- Support 3de lijn: Proximus
- Setup: 2/3 maand

Kostprijsregeling

- Geen upfront investering nodig, enkel een maandelijkse fee (HW, SW en diensten inbegrepen)
- 2 grote modules: Basic + opties
- vaste prijs per user per jaar (in blokken van 100 gebruikers)

Wat is de voorziene verdere evolutie van de dienst ?

- De dienst zal de productevoluties en verbetering volgen die worden aangebracht door de leverancier tijdens de duur van het contract. Het contract laat toe om technologische evoluties en/of productwijzigingen door te voeren.

Praktische info

- Raamovereenkomst beschikbaar voor alle FODS voor periode van 7 jaar (instap binnen eerste 4 jaar)
- Instap bij minimale afname van 3 jaar