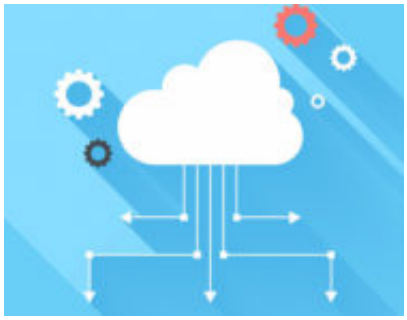
SPC Cloud: le best practice cloud security per il sistema Cloud Computing italiano

Date : 4 aprile 2017



Introduzione

Forse non tutti sanno che nel 2016 è stata aggiudicata la più grande gara europea relativa alla realizzazione della nuova piattaforma digitale nazionale, secondo il paradigma cloud computing, per la Pubblica Amministrazione italiana denominata “SPC Cloud”[1]

La gara SPC Cloud è di fatto un passo importante nell’attuazione della strategia ICT nazionale come indicato nel documento “Strategia per la crescita digitale 2014-2020” della Presidenza del Consiglio[2] .

In particolare, il progetto, del valore complessivo di quasi 2 miliardi di euro, è stato suddiviso in 4 lotti, due dei quali riferiti alla realizzazione dell’infrastruttura e servizi IaaS, PaaS e SaaS (Lotto 1, valore di 500 Milioni di euro) e sulle soluzioni e servizi di sicurezza (Lotto 2, valore di 600 Milioni di euro)

Perché è importante far conoscere ad un ampio pubblico questo progetto?

In primo luogo perché si tratta di un progetto di trasformazione, coordinata, delle infrastrutture e servizi ICT di tutta la PA (locale, regionale, centrale,…) secondo un’architettura e linee guida definite secondo il paradigma Cloud Computing . Consip (Centrale di committenza nazionale degli acquisti nella PA)[3], Agid (Agenzia per l’Italia Digitale) ed i fornitori aggiudicatari del contratto hanno predisposto dei siti web specifici (“Portali di governo e gestione della fornitura”) [4] [5] in cui vengono descritte tutte le informazioni del contratto quadro, in particolare le descrizioni tecniche dei servizi offerti ed i relativi listini prezzi.

La “trasparenza” degli aspetti tecnico-commerciali è sicuramente una novità per questo tipo di contratti per la PA e consente a tutti gli attori del mercato, non soltanto i referenti del contratto, di conoscere sia come viene descritto un servizio innovativo “security as a service” sia come quotarlo.

Da questo punto di vista i contenuti dei due portali possono offrire un insieme di “best practice”

su come costruire ed offrire un servizio cloud computing e quindi consentire sia agli operatori dell'offerta di migliorare le proprie proposizioni tecnico-commerciali sia al mercato della domanda di utilizzare le stesse informazioni come "benchmark" per capire meglio come definire dei requisiti tecnici per le proprie esigenze e percorsi di trasformazione in cloud di servizi e infrastrutture.

Ma facciamo un breve focus sul portale di governo e gestione della fornitura dei servizi di "sicurezza as a service", area di interesse della nostra Rubrica.

SPC Cloud Security

Nell'ambito del Contratto Quadro vengono erogati le seguenti categorie di servizi di sicurezza[6]:

1. servizi per la gestione delle identità digitali, erogati in modalità "as a service" (servizio IAM)
2. servizio di firma digitale remota comprensiva della fornitura di certificati e servizio di timbro elettronico, erogati in modalità "as a service", volti a favorire la dematerializzazione dei documenti e la digitalizzazione dei processi amministrativi
3. ?servizi di sicurezza, erogati sia in modalità "as a service" attraverso i Centri Servizi del Fornitore sia in modalità "on premise", atti a garantire la sicurezza applicativa e a supportare le Amministrazioni nella prevenzione e gestione degli incidenti informatici e nell'analisi delle vulnerabilità dei sistemi informativi. Includono anche servizi professionali a supporto delle attività delle Unità Locali di Sicurezza o strutture equivalenti delle Pubbliche Amministrazioni

In particolare, le soluzioni tecnologiche proposte in modalità *as a service* sono suddivise nelle seguenti sotto-categorie:

- Identity & Access Management (I&AM)
- Firma digitale remota
- Timbro elettronico
- Static application security testing
- Dynamic application security testing
- Mobile application security testing
- Vulnerability assessment
- Data loss/leak prevention
- Database security
- Web application firewall management e next generation firewall management
- Secure web gateway

In ognuna delle sotto-categorie sono stati predisposti dei *datasheet* strutturati nel modo seguente:

- Introduzione generale sul servizio proposto con indicazione dei livelli di criticità

- Gestione degli incidenti e tempistica
- Descrizione dettagliata del servizio, architettura e componenti tecnologiche (prodotti)

Le soluzioni vengono erogate attraverso “Centri Servizi” di proprietà del Fornitore, dislocati su sedi (data center) ubicate sul territorio comunitario e certificate ISO 27001. Il Fornitore del servizio è inoltre tenuto a trattare, trasferire e conservare le eventuali repliche dei dati conservati dai suddetti Centri Servizi sempre all’interno del territorio comunitario.

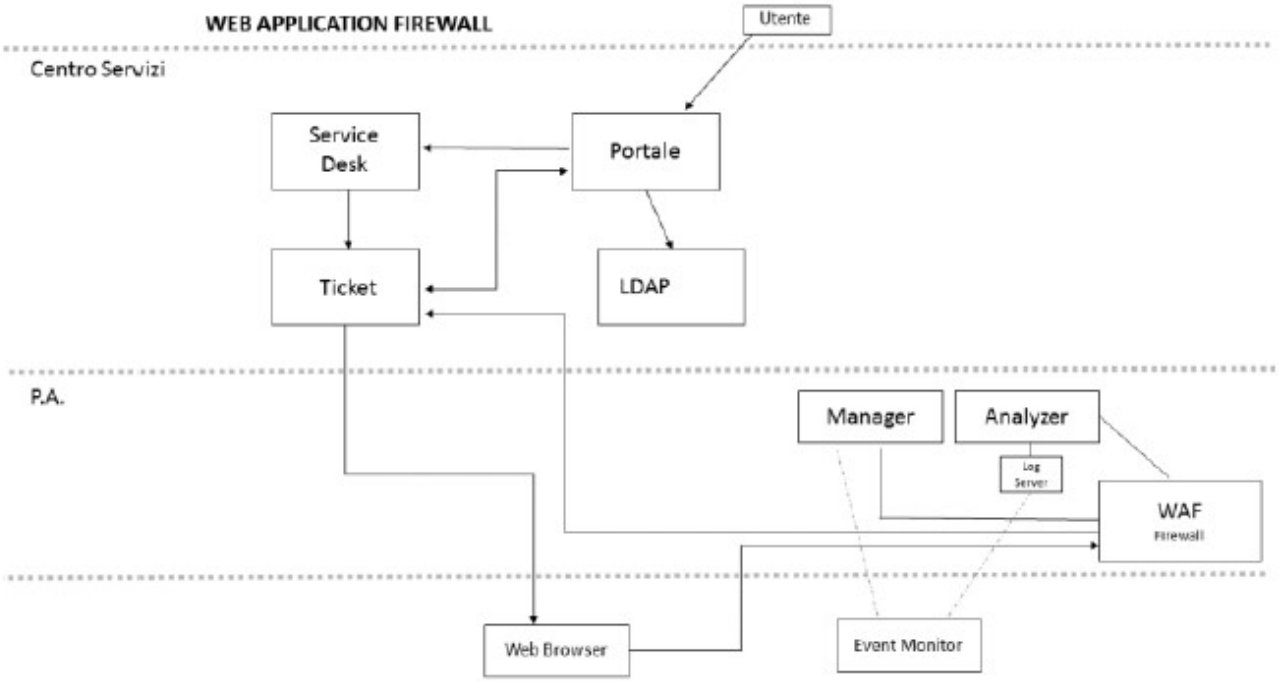
Un esempio di servizio SPC Cloud Security: Web application firewall management e next generation firewall management[7]

Il servizio proposto consente alla PA di proteggere le applicazioni web da attacchi esterni agendo da filtro del traffico dati a livello applicativo, superando quindi le caratteristiche dei classici Intrusion Detection System (IDS).

Il servizio si compone delle seguenti funzionalità:

- funzionalità standard firewall (policy enforcement, stateful inspection, packet filtering, NAT, VPN client-to-site e site-to-site);
- anti-malware e anti-spam;
- Intrusion Prevention (IPS) per il blocco delle minacce;
- monitoraggio del livello di sicurezza degli applicativi web;
- prevenzione avanzata contro le intrusioni e filtraggio dei contenuti;
- deep packet inspection per scansionare l'intero payload dei pacchetti;
- produzione di report personalizzabili di sintesi (executive summary) e di dettaglio (technical report) e compliance

L’architettura di riferimento è la seguente:



L’architettura è dislocata presso:

- Centro Servizi;
- Pubblica Amministrazione (previa allocazione di spazi attrezzati, rack, ecc.).

Presso il Centro Servizi sono dislocati:

- Portale dei Servizi di Sicurezza: per effettuare nuove richieste di servizi (es.: creazione o modifica di una policy)
- LDAP: per l’accesso ai servizi con utenza di dominio
- Service Desk / Ticket: piattaforma di ticketing per la gestione delle richieste
- Event Logs: per la raccolta di tutti gli eventi

Conclusioni

Spesso evidenziamo le difficoltà (abitudine Italica!) del mercato della sicurezza informatica nazionale legate alla indisponibilità di budget sufficienti e progetti sfidanti/innovativi. Il progetto SPC Cloud, nonostante sia stato gestito come un “classico” contratto quadro ICT della Pubblica Amministrazione, si sta rivelando invece un ottimo “esercizio”, prima di tutto per i fornitori, nel presentare servizi di cloud security ” trasparenti” (in termini di SLA, costi, …) , disegnati per rispondere alla maggior parte delle esigenze di sicurezza di clienti piccoli , medi e grandi (con riferimento rispettivamente alla Pubblica Amministrazione Locale, Regionale e Centrale).

L’aspetto interessante del modello di erogazione utilizzato è la somiglianza al nascente modello Cloud Access Security Broker (CASB), di cui abbiamo già parlato in un recente articolo della nostra rubrica, che costituirà nei prossimi anni un importante modello di business nel mercato Security as a Service (o SecaaS).

Tutte queste informazioni sono accessibili liberamente da tutti gli operatori del mercato (cittadini inclusi) e quindi a supporto di una migliore conoscenza e (ri)utilizzo delle migliori best practice di cloud security.

Infine, CSA Italy ed Agid hanno deciso di avviare una collaborazione volta alla realizzazione di una serie di seminari specifici su SPC Cloud (il primo dei quali si svolgerà il prossimo 13 Aprile a Roma[8]) a supporto di una più ampia ed efficace divulgazione delle potenzialità ed opportunità offerte da questo progetto non solo per la Pubblica Amministrazione ma anche per l’intero mercato ICT (e Cloud) nazionale.

[1] http://www.consip.it/news_ed_eventi/2016/7/notizia_0019

[2] http://www.agid.gov.it/sites/default/files/documenti_indirizzo/crescita_digitale_nov_2014.pdf

[3] http://www.consip.it

[4] https://www.cloudspc.it/

[5] https://www.spc-lotto2-sicurezza.it/

[6] https://www.spc-lotto2-sicurezza.it/wps/portal/spc_pdg/contratto_quadro/!ut/p/z1/

[7] https://www.spc-lotto2-sicurezza.it/wps/PDGWCMJSPs/jsp/html/PdfSchedaServizio.jsp?codice=L2.S3.7

[8] http://cloudsecurityalliance.it/workshop-csa-agid-spc-cloud-e-la-sicurezza-del-sistema-cloud-computing-nazionale-13-aprile-roma/

A cura di: **Alberto Manfredi**