Contratto Quadro SPC Cloud Lotto 1

Servizi di sicurezza - DDoS

Piano di Attivazione

Gestione	Azienda	Riferimento
REDATTO:	Telecom Italia S.p.A.	
REDATTO:	DXC Technology	
APPROVATO:	Telecom Italia S.p.A. (Mandataria), DXC	
N° allegati:	0	

Telecom Italia S.p.A.
(ing. Giovanni Santocchia)

Firmato digitalmente da:
GIOVANNI SANTOCCHIA
Telecom Italia S.p.A./00488410010
Firmato il 22/04/2019 22:11
Seriale Certificato: 443651
Valido dal 05/12/2016 al 05/12/2019
TI Trust Technologies CA

INDICE

1. REGISTRAZIONE MODIFICHE DOCUMENTO

N° Rev.	Descrizione	Data emissione
0	Prima emissione	04/02/2019

2. GENERALITA'

2.1. Applicabilità

Il documento si applica nell'ambito del Contratto Quadro SPC Cloud Lotto1.

2.2. Assunzioni

Non applicabile.

2.3. Riferimenti

Identificativo	Titolo/Descrizione
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5B Capitolato Tecnico
Gara Cloud Lotto 1	Gara Cloud Lotto 1_Allegato 5A Capitolato Tecnico Parte Generale
Gara Cloud Lotto 1	Offerta Tecnica del Fornitore Allegato B Relazione Tecnica Lotto 1

2.4. Definizioni ed Acronimi

Definizioni/Acronimi	Descrizione
IaaS	Infrastructure as a Service
PaaS	Platform as a Services
RTI	Raggruppamento temporaneo d'Impresa
DDoS	Distributed Denial of Service
ISP	Intenet Service Provider
GRE	Generic Routing Encapsulation
IP	Internet Protocol
PA	Pubblica Amministrazione
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività

3. ATTIVAZIONE DEL SERVIZIO

Nei capitoli successivi sono riportate le attività che devono essere svolte per consentire alle Amministrazioni l'attivazione del servizio DDoS al fine di proteggere i propri sistemi ospitati presso i Centri Servizi del RTI, nell'ambito della convenzione SPC Cloud Lotto 1.

Il servizio DDoS, fornito in modalità "Reattiva" e con copertura H24, è applicabile esclusivamente ai sistemi attivati dall'Amministrazione nei Centro Servizi della RTI nell'ambito SPC Lotto 1 ed esposti su Internet mediante la connettività condivisa presente presso i suddetti Centri Servizi ed utilizzata dalle Amministrazioni che hanno contrattualizzato i servizi infrastrutturali previsti dal Lotto 1.

3.1. Piano dei fabbisogni

L'attività indispensabile per l'implementazione del servizio DDoS è la definizione da parte della specifica Amministrazione del proprio Piano dei Fabbisogni.

L'Amministrazione quindi effettuerà l'analisi del proprio ambiente ovvero, individuerà gli IP ed i servizi associati da voler proteggere. L'attività di analisi potrà essere svolta dall'Amministrazione col supporto del team di progettazione messo a disposizione dal RTI in modo da facilitare le verifiche preliminari. Il team di progettazione opererà prevalentemente da remoto.

Terminata la fase di analisi l'Amministrazione procederà a definire il Piano dei Fabbisogni.

Una volta ricevuto il Piano dei Fabbisogni, il team di Progettazione predisporrà il Progetto dei Fabbisogni.

Il Piano dei Fabbisogni dovrà contenere le informazioni riportate nella check-list descritta di seguito.

3.1.1. Check List per servizio DDoS

Di seguito sono riportate le informazioni che devono essere riportate nel Piano dei Fabbisogni necessarie per le verifiche di fattibilità del servizio DDoS.

Elenco Informazioni da fornire

- *Sede Cliente*: indicare il Centro Servizi presso cui sono attivi i sistemi Cliente da proteggere realizzati mediante le risorse IaaS (VM e VDC) e/o PaaS previste dalla convenzione SPC Cloud Lotto 1;
- *Subnet pubbliche Cliente da rendere proteggibili*: devono essere indicati tutti gli IP e subnet che devono essere proteggibili mediante il servizio DDoS. Si ricorda che gli IP dei singoli host da proteggere devono essere annunciati su rete Internet mediante una subnet e non mediante indirizzo specifico;
- *Valore in Mb/s della banda da riconsegnare in caso di attacco*: tale valore deve essere scelto tra quelli proposti ed indicati nel documento "Servizi di sicurezza - DDoS - Specifiche del servizio" ad eccezioni delle soluzioni realizzate su base progetto;
- *IP pubblico "non Protetto da sistemi di sicurezza" per test di collaudo*: tale IP sarà utilizzato per effettuare il collaudo del servizio. L'IP di test deve esporre un servizio interattivo - http, https, ftp,…- o almeno rispondere al ping;
- *Elenco dei servizi Cliente da proteggere*: di seguito si riporta una tabella di esempio delle informazioni che devono essere fornite per ciascun servizio da proteggere:

Servizio/i Cliente protetti dal Ddos di TI	***Protocollo (udp/tcp)***	***Porta (esempio: 9999, 443 (https), 80 http)***	***IP Pubblico, Range IP Address***	***Network/Netmask (assegnate al Cliente) a cui l'IP pubblico,Range Address fanno riferimento***
Navigazione-Proxy			x.x.x.x	x.x.x.0/24
DNS			y.y.y.y-d.d.d.d	y.y.0.0/16
WEB Server			v.v.v.v	v.v.v.32/28
Altro			c.c.c.c	c.c.c.0/29

3.2. Progetto dei fabbisogni

Il team di Progettazione del RTI, ricevuto dall'Amministrazione il documento Piano dei Fabbisogni, provvederà a far verificare dalle proprie strutture tecniche la fattibilità del servizio e a seguito di riscontro positivo predisporrà il documento Progetto dei Fabbisogni.

Il documento Progetto dei Fabbisogni sarà quindi consegnato all' Amministrazione.

Il suddetto documento conterrà:

- Costi previsti per la realizzazione del servizio DDoS;
- Pre-fattibilità della soluzione con indicazione di massima degli IP/applicazioni che potranno essere protetti;
- Sintetica descrizione di come sarà implementato il servizio nello specifico ambiente dell'Amministrazione.
- Indicazione delle eventuali giornate di Cloud Enabling necessarie all'attivazione del servizio
- Tempi necessari all'attivazione del servizio

L'Amministrazione potrà richiedere la modifica/aggiornamento del Progetto dei Fabbisogni ogni qualvolta questa lo ritenga necessario. Le richieste che determinano modifiche/aggiornamenti del Progetto dei Fabbisogni saranno sempre oggetto di verifica tecnica.

3.3. Progetto esecutivo

Il progetto esecutivo sarà redatto dal personale del RTI a valle della formalizzazione del contratto esecutivo con l'Amministrazione.

Nel progetto esecutivo saranno indicati:

- gli IP/Applicazioni che saranno protetti con il servizio DDoS,
- le attività che saranno svolte per l'attivazione del servizio,
- elenco dei test che saranno svolti per il collaudo del servizio.

Il progetto esecutivo, previa condivisione preliminare dei contenuti con l'Amministrazione, sarà consegnato alle strutture di Delivery del RTI affinché si possa procedere all'implementazione del servizio stesso.

3.4. Implementazione del servizio

L'implementazione del servizio richiede che venga configurato il tunnel GRE tra il router infrastrutturale presente presso il Centro Servizi del RTI aggiudicataria della convenzione SPC Cloud Lotto 1 in cui sono ospitati gli ambienti dell'Amministrazione e l'apparato presente nella Security Farm TIM verso la quale sarà reinstradato il traffico in caso di attacco DDoS.

Durante la fase di implementazione del servizio verrà definita:

- la lista dei referenti dell'Amministrazione autorizzati a richiedere l'attivazione del servizio DDoS Mitigation.
- La lista dei referenti del SOC del RTI autorizzati sia a ricevere le richieste, fatte dal personale dell'Amministrazione autorizzato, di attivazione del servizio di DDoS Mitigation sia a procedere all'attivazione dello stesso.

Per i referenti sopra citati (sia Cliente sia del SOC) dovranno pertanto essere forniti i seguenti dati: nome cognome, mail, telefono e cellulare.

Tali informazioni saranno riportate in un file excel che sarà fornito all'Amministrazione, all' Help Desk del RTI ed al SOC. Verranno inoltre forniti all'Amministrazione i template delle mail che dovranno essere scambiate per richiedere l'attivazione del servizio DDoS Mitigation e nelle fasi successive come descritto nel parg.3.6.2 "Specifiche per l'invio delle mail" del documento SPC Cloud LT1 Servizi di Sicurezza DDoS – Specifiche funzionali".

L'attività sarà effettuata a valle del caricamento sui sistemi di Governance del nuovo profilo di servizio che l'Amministrazione avrà contrattualizzato.

Al termine delle attività di implementazione del servizio verrà effettuato il collaudo.

I tempi necessari all'attivazione del servizio saranno riportati nel Progetto dei Fabbisogni.

3.5. Collaudo

Terminata l'implementazione del servizio per la singola Amministrazione sarà effettuato un collaudo atto a verificare il corretto funzionamento del servizio stesso.

I test di collaudo saranno concordati con l'Amministrazione e saranno descritti in apposite schede predisposte durante la fase di attivazione del servizio. Nelle schede sarà riportato l'esito del test stesso. In caso di esito negativo nella scheda tecnica sarà riportato il livello di gravità (bloccante, grave, accettabile) riscontrato.

Il collaudo si ritiene superato solo nel caso in cui non siano presenti anomalie classificate come gravi o bloccanti.

Per il collaudo del servizio sarà utilizzato un IP di test non protetto precedentemente fornito dall'Amministrazione. Tale IP di test dovrà esporre un servizio interattivo -http, https, ftp,…- o almeno rispondere al ping. L'IP utilizzato per i test non dovrà esporre servizi critici inquanto potrebbero verificarsi, solo per l'IP di test, indisponibilità del servizio durante l'esecuzione dei test stessi.

In presenza di anomalie gravi e/o bloccanti, a seguito dell'analisi che verrà effettuata, verranno intraprese dalle parti le azioni correttive e si procederà ad una nuova programmazione del collaudo.

Di seguito si riporta un esempio di scheda di test:

Campo	Significato
Requisito	Identificativo del requisito oggetto del test
Scopo	Riassume l'obiettivo del test
Modalità di esecuzione	Indica la modalità di esecuzione del test, ad esempio per accesso diretto alla piattaforma, iniziando dall'accesso
Scenario di riferimento	Descrive lo 'scenario utente' nel quale avviene il test e le condizioni che caratterizzano lo scenario
Macro azioni	Sono i passi operativi che si compiono durante la rappresentazione del test.
Risultato atteso	E' lo scenario utente atteso, a seguito dell'esecuzione del test.
Esito del test	E' l'esito del test, positivo se lo scenario ottenuto a seguito del test coincide con lo scenario atteso, negativo in caso contrario.

Di seguito è riportato un esempio dei test da effettuare per il collaudo del servizio:

- verificare la raggiungibilità del servizio esposto sull'IP di test
- verifica di rete in 'peace time' sull'IP di test (annuncio BGP, traceroute)
- attivazione protezione per l'IP di test
- verifica di rete in 'war time' sull'IP di test (annuncio BGP, traceroute)
- verificare l'attivazione mitigation sulla piattaforma Arbor
- verificare la raggiungibilità del servizio esposto sull'IP di test
- ***[opzionale]*** configurazione contromisura sulla piattaforma Arbor atta a bloccare "traffico di attacco"
- ***[opzionale]*** iniziare generazione "traffico di attacco"
- ***[opzionale]*** verificare raggiungibilità del servizio esposto sull'IP di test
- ***[opzionale]*** verificare efficacia della contromisura sulla piattaforma Arbor
- ***[opzionale]*** interrompere la generazione "traffico di attacco"
- disattivazione protezione per l'IP di test
- verificare la disattivazione mitigation sulla piattaforma Arbor
- verificare la raggiungibilità del servizio esposto sull'IP di test
- verifica di rete in 'peace time' sull'IP di test (annuncio BGP, traceroute)

Le attività indicate come ***opzionale*** sono solitamente svolte a meno della presenza di condizioni che non le rendano possibili/utili. Si precisa che in ogni caso il "traffico di attacco" generato durante i test è sempre un traffico generato dallo RTI tale da non causare normalmente alcun impatto generalizzato né sulla connettività Cliente né sugli eventuali altri servizi esposti dal Cliente.

Come indicato sopra i test di collaudo saranno effettuati utilizzando un IP di test fornito dal Cliente. Tale IP IP non dovrà esporre servizi critici in quanto durante i test di collaudo non si può escludere a priori il verificarsi di qualche disservizio su tale IP di test.

La durata del collaudo verrà definita con ciascuna Amministrazione sulla base dei test concordati, comunque in generale il tempo necessario al collaudo è pari indicativamente a 1 giorno lavorativo.

Al termine con esisto positivo del collaudo sarà comunicato al referente dell'Amministrazione l'avvio del servizio DDoS mediante una "welcome letter".