Contratto Quadro SPC Cloud Lotto 1

Servizi di Sicurezza - DDoS

Specifiche del Servizio

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 DEL DOCUMENTO 3
2 GENERALITA' 4
2.1 Applicabilità 4
2.2 Assunzioni 4
2.3 Riferimenti 4
2.4 Definizioni ed Acronimi 4
3 SERVIZIO DDoS PROTECTION 5
3.1 Requisiti e applicabilità 5
3.2 Architettura Generale 6
3.2.1 Architettura del servizio 7
3.3 Modello di servizio 9
3.4 Test periodici 10
3.5 Risorse Utilizzate 10
3.6 Processi a supporto per l'erogazione del servizio 10
3.6.1 Flusso procedurale per attivazione "diversion" 10
3.6.2 Specifiche per l'invio delle mail. 11
3.6.3 Descrizione delle fasi per gestione attacco DDoS. 12

1 REGISTRAZIONE MODIFICHE DEL 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 alle soluzione IaaS e PaaS.

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
DDoS	Distributed Denial of Service
ISP	Intenet Service Provider
DC	Data Center
GRE	Generic Routing Encapsulation
IP	Internet Protocol
PA	Pubblica Amministrazione
RTI	Raggruppamento Temporaneo d'Impresa
SOC	Security Operation Center
SPC	Sistema Pubblico di Connettività

3 SERVIZIO DDOS PROTECTION

In questo capitolo sono descritte le funzionalità del nuovo servizio infrastrutturale di sicurezza, denominato DDoS (Distributed Denial of Service) che l' RTI aggiudicatario dei servizi di Cloud Computing oggetto del Lotto 1 propone quale servizio aggiuntivo di cui potranno fruire le Amministrazioni.

Tale servizio va ad aggiungersi ed integrarsi con quelli già previsti e richiesti dalla procedura di Gara per andare incontro alle esigenze delle Pubbliche Amministrazioni.

Il servizio di DDoS Protection offerto dal RTI garantisce la mitigazione degli attacchi DDoS provenienti da rete Internet e diretti ai server attivati dalle Amministarzione nell'ambito della convenzione SPC Lotto 1 e pertanto ubicati nei Centri Servizi del RTI aggiudicataria della suddetta convenzione.

Allo scopo di proteggere il proprio IP backbone pubblico da attacchi di tipo DDoS (DDoS Mitigation Infrastrutturale), TIM ha predisposto già da alcuni anni una piattaforma dedicata. Tale piattaforma è stata quindi personalizzata per poter offrire il servizio di DDoS Mitigation anche ai Clienti finali. Tale piattaforma, sarà utilizzata per fornire il servizio DDoS alle Amministrazioni che utilizzano i servizi infrastrutturali presenti nel Lotto 1.

La tipologia di attacco contrastata dal servizio offerto è il "Volumetric Attack" che mira alla saturazione del link di collegamento mediante la generazione di altissimi volumi di traffico e rendendo indisponibile il sistema del Cliente. Tale tipologia di attacco è generalmente generato da:

- botnet (reti di computer/server compromessi mediante malware e in possesso degli attaccanti),
- server in hosting con alta capacità di generazione traffico in banda,
- server/servizi che vengono abusati per generare traffico anomalo sfruttando debolezze dei protocolli esposti (DDoS Relection & Amplification),
- redirezione di traffico di navigazione da client leciti mediante compromissione di siti e banner pubblicitari,
- infrastrutture DDoSaaS (Distributed Denial of Service as a service anche dette Booter/Stresser) che consentono di lanciare attacchi di diversa tipologia previa pagamento di un abbonamento).

Il contrasto efficace di questo tipo di attacchi, per la loro stessa natura, può essere realizzato esclusivamente proteggendo le risorse trasmissive che forniscono la connettività Internet. Nel caso di attacchi DDoS la protezione risulta tanto più efficace quanto più è realizzata in prossimità delle sorgenti degli attacchi e quindi lontano dai target. Per tale motivo una protezione ottimale può essere realizzata solo ed esclusivamente nell'infrastruttura dell'operatore di TLC che fornisce il servizio di connettività.

Il servizio è proposto con copertura H24 in modalità "reattiva" ovvero sarà l'Amministrazione a contattare la struttura di riferimento della RTI (Help Desk~~Security Operation Center – SOC~~) al verificarsi di un attacco o qualora l'Amministrazione ritenga si stia verificando un attacco.

Il servizio dovrà avere una durata contrattuale minima di un anno.

3.1 Requisiti e applicabilità

Il servizio DDoS è reso disponibile alle Amministrazioni al fine di proteggere esclusivamente i sistemi virtuali di tipo IaaS (VM e VDC) e PaaS acquisiti nell'ambito della convenzione SPC Cloud Lotto 1.

Il servizio è applicabile esclusivamente alla connettività Internet condivisa fornita dalla RTI presso i propri Centri servizi nell'ambito della convenzione SPC Cloud Lotto 1 ed utilizzata dalle Amministrazioni che hanno contrattualizzato i servizi infrastrutturali previsti dal Lotto 1.

Il servizio non è applicabile alla connettività INFRANET poiché quest'ultima è realizzata mediante una VPN MPLS.

Nello specifico il servizio DDoS Protection protegge esclusivamente IP pubblici esposti su Internet da attaccanti che siano in Internet, pertanto eventuali attacchi provenienti dalla rete INFRANET non sono né rilevabili né gestibili.

Si evidenzia comunque che la rete INFRANET, essendo realizzata tramite VPN MPLS, si configura come una rete segregata con accessi dedicati alle sedi della PA e pertanto non raggiungibile da rete Internet.

Per l'applicazione del servizio devono essere soddisfatti il seguenti pre-requisiti:

- l'Aministrazione deve avere acquistato risorse IaaS (VM e VDC) e/o Paas nell'ambito della convenzione SPC Cloud Lotto 1;
- i sistemi che possono essere protteti sono tutti e soli quelli realizzati con le risorse IaaS (VM e VDC) e/o PaaS acquistate nell'ambito della convenzione SPC Cloud Lotto 1 e quindi ubicati presso i Centri Servizi del RTI;
- i sistemi da protteggere devono essere annunciati sulla rete Internet esclusivamente tramite gli accessi Internet forniti dal RTI nell'ambito della convenzione SPC Cloud Lotto 1 e pertanto presenti esclusivamente presso i Centri Servizi del RTI. Inoltre l'annuncio di suddetti sistemi deve essere fatto a livello di subnet e non di singolo host (non sono ammessi annunci con indirizzi /32);
- il traffico analizzato e prottetto è esclusivamente quello indirizzato tramite rete Internet verso i sistemi indicati dall'Amministrazione e ubicati presso i Centri Servizi del RTI aggiudicataria della convenzione SPC Cloud Lotto 1. Conseguentemente viene esclusa l'analisi e la protezione del traffico proveniente da rete Internet e diretto verso indirizzi IP diversi da quelli configurati per ciascuna Amministrazione a livello subnet sulla piattaforma Openstack.

3.2 Architettura Generale

L'infrastruttura che eroga il servizio di protezione è posizionata all'interno del backbone IP pubblico di TIM.

Questo ambiente rappresenta un sistema autonomamente consistente nella gestione dei protocolli di routing e ciò rende particolarmente efficace l'interazione tra gli apparati di rete che compongono il backbone e quelli dedicati al servizio di protezione, permettendo la variazione dinamica dei flussi di traffico che è alla base dei meccanismi di reazione alla presenza di un attacco DDoS.

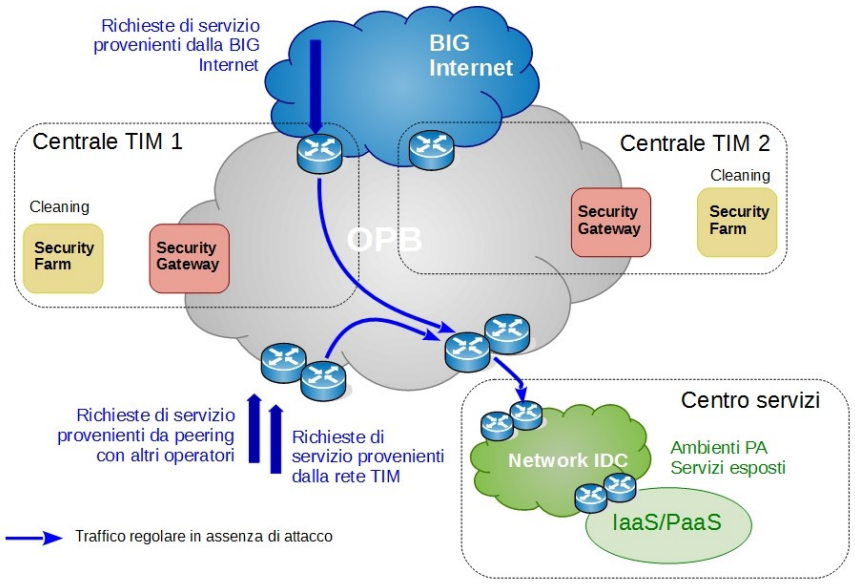
Le tecnologia scelta per l'implementazione del servizio è Arbor Networks, leader di mercato.

All''interno dell' infrastruttura di rete TIM sono state definite alcune aree di "cleaning", dette Security Farm, interamente ridondate, dedicate all'erogazione del servizio DDoS.

La posizione delle Security Farm è stata individuata anche in funzione della vicinanza ai punti di interconnessione internazionale dai quali provengono la maggior parte degli attacchi.

In condizione di normale erogazione dei servizi sulla rete pubblica, i flussi di traffico vengono gestiti dal backbone IP e indirizzati al centro servizi nel quale sono ospitati i sistemi destinazione. Nel caso specifico il traffico è indirizzato verso i sistemi realizzati dalle Amministrazione nei Data Center dello RTI mediante i servizi IaaS (VM e VDC) e/o PaaS acquisiti nell'ambito della convenzione SPC Cloud Lotto 1.

La figura seguente mostra in generale l'architettura di funzionamento in assenza di attacchi.



Rappresentazione dell'architettura di prevenzione del DDoS in assenza di attacchi

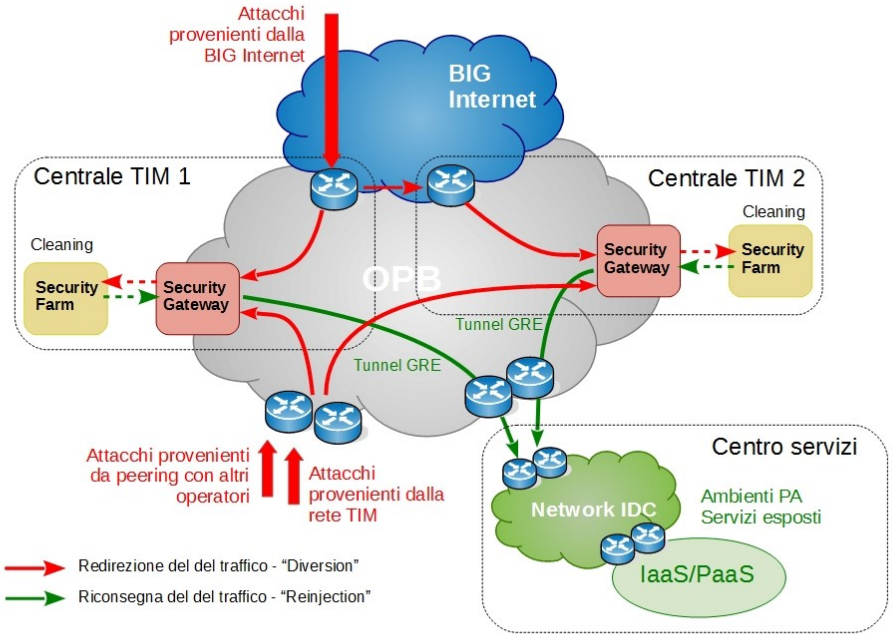
3.2.1 Architettura del servizio

Il servizio di DDoS Protection offerto prevede una gestione "reattiva" con copertura H24. Sarà pertanto la stessa Amministrazione a segnalare allo SPOC del RTI che i propri sistemi, presenti nei Centri Servizi dello RTI ed esposti su Internet, sono anche solo presumibilmente oggetto di un attacco.

L'attività di contrasto ad un attacco di tipo DDoS, a valle della segnalazione da parte del Cliente, è composta da tre fasi distinte:

- Diversion
- Cleaning
- Re-injection

La figura seguente mostra lo schema generico di funzionamento del servizio in caso di attacco.



Rappresentazione dell'architettura di prevenzione del DDoS in presenza di attacchi

Di seguito sono dettagliate le tre fasi sopra indicate:

- Diversion: Il Security Operation center (SOC) dello RTI attiva la redirezione del traffico Cliente riferito all'IP o agli IP sotto attacco verso le Security Farm con l'obiettivo di analizzare i flussi di traffico sotto attacco e intraprendere le azioni di cleaning. La redirezione dei flussi di traffico sotto attacco è realizzata attraverso l'iniezione di specifiche rotte attraverso i protocolli di routing dinamico della rete di telecomunicazione di TIM con l'obiettivo di forzare il transito verso le Security Farm.
- Cleaning: A seguito della diversion, il traffico è consegnato all'apparato di cleaning che analizzerà la tipologia dell'attacco e applicherà tutte le misure necessarie ad eliminare la sola componente indesiderata del traffico. Al termine delle attività di pulizia, il solo traffico legittimo è riconsegnato al Cliente attraverso la funzionalità di Re-Injection.
- Re-Injection: Il traffico legittimo viene riconsegnato al Cliente attraverso un tunnel GRE chiuso tra le Security Farm ed i router di attestazione del centro servizi che ospita i sistemi oggetto di attacco. Nello specifico il tunnel verrà chiuso sul router infrastrutturale del Centro Servizi della convenzione SPC Cloud Lotto 1 presso cui sono posizionati i sistemi Cliente sul quale è terminata la connettività internet. La modalità Tunnel GRE assicura che il traffico sia instradato in maniera puntuale.

La fase di Cleaning rappresenta la fase nevralgica del servizio ed è caratterizzata dai seguenti step:

- Attivazione di filtri dinamici: sono utilizzate sia delle regole statiche di base per riconoscere il tipo di attacco DDoS, sia eventuali ulteriori filtri dinamici inseriti in tempo reale dagli specialisti del SOC.
- Verifica dello Spoofing IP: sono previsti meccanismi di Source Verification per individuare indirizzi IP Spoofed ed evitare che il traffico legittimo venga erroneamente catalogato come Spoofed.
- Analisi del traffico: in questa fase si analizza il traffico ripulito nelle fasi precedenti, esaminando il flusso in base al protocollo ed alla sorgente/destinazione, individuando variazioni sospette rispetto al

comportamento standard desunto dai dati acquisiti. In caso di rilevamento di nuovi attacchi, sono scatenati gli alert preventivamente definiti ed eventualmente attivati ulteriori filtri dinamici del traffico.

- Analisi di protocollo: in questa fase sono identificati gli attacchi legati a specifiche applicazioni o protocolli, come ad esempio errori o transazioni incomplete HTTP.
- Gestione della banda: in questa fase, infine, viene filtrato in maniera controllata il traffico ritenuto legittimo, in modo da non sovraccaricare, in ogni caso, il sistema target.

Il servizio di DDoS Protection prevede, nel caso di attacco, una modifica nelle tabelle di routing nel backbone di TIM relativamente agli IP pubblici del Cliente sotto attacco. In tal modo viene effettuata, da parte del SOC, la Diversion del traffico 'legittimo e malizioso' del Cliente verso le Cleaning Farm attestate sulla rete TIM.

Per tutta la durata dell'attacco il personale del SOC è costantemente impegnato a monitorarne l'evoluzione.

Una volta terminato l'attacco, e solo in accordo con il Cliente, si procede ad interrompere la diversion, consentendo al traffico di seguire la strada tradizionale.

Ad attività terminata, ovvero effettuata la disattivazione della diversion, il SOC redige ed invia un Incident Report, contenente i dettagli di quanto rilevato. Il Report verrà consegnato al Cliente nelle tempistiche riportate nel documento "Specifiche di Controllo".

3.3 Modello di servizio

Il servizio permette di analizzare e eventualmente mitigare attacchi DDoS su un volume di traffico Cliente fino a 160 Gbps, assicurando all'Amministrazione la riconsegna del traffico lecito per il taglio di banda contrattualizzato. I tagli di banda riconsegnata che possono essere contrattualizzati dalal Amministrazione sono riportati nella tabella seguente:

Banda Riconsegnata Mbps
10
30
60
100

La scelta del profilo di banda Internet riconsegnata dipende dal volume medio di traffico sviluppato per l'utilizzo dei servizi esposti su Internet.

Qualora l'Amministrazioen necessiti di un valore di banda riconsegnata maggiore di quelli indicati verrà valutata la fattibilità del servizio a progetto.

Il servizo DDoS Protection proposto dal RTI è caratterizzato inoltre dai seguenti elementi:

- MITIGATIONS: illimitate.
- TIPOLOGIA MITIGAZIONE: Reattiva, ovvero sarà il referente dell'Amministrazione a segnalare allo SPOC un sospetto attacco DDoS.
- DURATA ATTACCO: illimitata, ovvero non c'è un limite temporale per la durata della fase di "diversion".
- TEMPO PER ATTIVAZIONE DELLA DIVERSION: entro 30 minuti dall'apertura da parte dello SPOC del ticket sul sistema di Ticketing di SPC. Al ticket sarà allegata la mail di "Richiesta attivazione del servizio di DDoS Mitigation" inviata dal referente Cliente.
- INCIDENT REPORT: entro 2 giorni lavorativi dalla disabilitazione del servizo DDoS Mitigation.

- SECURITY OPERATION CENTER (SOC): presso di esso operano operatori specializzati che si occupano di analizzare gli attacchi ed attivare l a"diversion" del traffic. Il SOC èoperativo H24/365

3.4 Test periodici

All'attivazione del servizio verrà effettuato un test di collaudo del servizio stesso come meglio dettagliato nel documento "SPC Cloud Servizi di Sicurezza DDoS Piano di Attivazione".

Il servizio prevede inoltre che venga fatto con cadenza annuale un test finalizzato alla verifica della congruenza del servizio rispetto a quanto realizzato nella fase di attivazione.

3.5 Risorse Utilizzate

Il servizio DDoS Protection proposto dal RTI non prevede l'acquisizione di elementi Hardware o Software da parte dell'Amministrazione.

Le risorse utilizzate sono relative al personale del SOC che sarà coinvolto dal personale del Help-Desk (SPOC) a seguito di richiesta da parte del Cliente, al verificarsi di un attacco. Il personale del SOC provvederà se necessario a mettersi in contato con il referente dell''Amministrazione.

3.6 Processi a supporto per l'erogazione del servizio

Il servizio prevede che l'attività di contrasto (Mitigation) ad un attacco di tipo DDoS sia attivata, a seguito esclusivamente di una richiesta esplicita da parte dei referenti dell'Amministrazione. In fase di implementazione del servizio verranno individuti i referenti dell'Amminostrazione ed i referenti del SOC.

Nel seguito è descritto il processo operativo utilizzato per contrastare un attacco DDoS.

3.6.1 Flusso procedurale per attivazione "diversion"

Qualora il Cliente sospetti un attacco DDoS dovrà procedere come di seguito riportato.

1) il Cliente effettua una chiamata allo SPOC per richiedere l'attivazione della diversion a seguito di attacco o sospetto attacco DDoS e contestualmente invia la mail di "richiesta attivazione diversion" sia allo SPOC (l'indirizzo mail è quello già in uso per contattare l'Help-Desk) che al SOC (l'indirizzo mail sarà fornito in fase di attivazione del servizio).
   L'accesso allo SPOC avverrà in copertura H24 mediante una delel due modalità descritte:
   a) mediante chiamata al NV con inserimento del PIN dedicato specifico del Cliente per singolo contratto e contestuale invio di mail di richiesta attivazione diversion allo SPOC ed al SOC. La mail di richiesta attivazione della diversion sarà redatta secondo il formato che sarà comunicato al Cliente in fase di attivazione del servizio. Il PIN Cliente sarà caratterizzato come PIN associato ad un servizio con copertura H24.
   b) mediante apertura di un pre-ticketing sul sistema di sef-ticketing reso disponibile da SPC Cloud.
2) Lo SPOC prende in carico la chiamata ed apre la segnalazione sul TTM di SPC se il cliente ha chiamato al NV oppure prende in carico il pre-ticket (SD) sul TTM di SPC se il cliente ha aperto la segnalazione in Self Ticketing e successivamente tramuta il pre-ticket in Ticket sempre sul TTM di SPC. Con l'apertura del ticket sul sistema TTM di SPC parte il conteggio relativo al tempo di attivazione della diversion (tempo di inizio per il calcolo degli SLA). Contestualmente lo SPOC ingaggia il SOC. Nella richiesta di ingaggio del SOC sarà allegata la mail Cliente di richiesta attivazione diversion.

3) Il SOC prende in carico la richiesta ed effettua la fase di autenticazione ovvero verifica che il mittente della mail di "richiesta attivazione diversion" sia nell'elenco delle persone abilitate a richiedere tale servizio. Se la fase di autenticazione:
   a. ha esito negativo, il SOC invia una mail al richiedente Cliente segnalando che non è autorizzato a richiedere il servizo e contestualmente ne dà notifica allo SPOC che provvederà a chiudere il ticket sul sistema TTM di SPC Cloud indicando che il referente non è corretto. Il flusso termina qui.
   b. ha esito positivo, il SOC avvia la fase di veriifica di effettivo attacco DDoS, contattando eventualmente il referente Cliente tramite mail o chiamata telefonica. Si procede col punto successivo.
4) Se l'analisi:
   a. ha esito negativo, ovvero non viene riscontrato un attacco DDoS:
      i. il SOC notifica al referente Cliente e allo SPOC che l'evento non è riscontrato. Lo SPOC chiude il ticket sul sistema TTM di SPC Cloud indicando che non si è riscontrato alcun attacco DDoS. Il flusso termina qui.
   b. ha esito positivo: il SOC avvia all'interno le attività per l'attivazione della diversion, dandone notifica allo SPOC. Si procede coi punti successivi.
5) Il SOC una volta che la diversion è stata attivata ne dà notifica allo SPOC ed invia una mail al referente cliente. Lo SPOC chiude il ticket sul sistema. Con la chiusura del Ticket termina l'intervallo temporale sul quale viene calcolato lo SLA per l'attivazione della "diversion" (max 30 min.).
6) Il processo di disattivazione della diversion sarà gestito senza intervento dello SPOC e senza tracciamento sul sistema di Trouble Ticketing di SPC Cloud; si effettuerà solo uno scambio di mail tra referente Cliente e referente SOC. Le mail scambiate avranno il formato che sarà comunicato al Cliente in fase di avvio del servizio, in pratica il formato usato per i Clienti Mercato.
7) Entro 2 giorni lavorativi dalla disattivazione della diversion il SOC fornirà l'Incident Report. Lo SLA relativo ai 2 giorni sarà consuntivato manualmente ed inserito sul sistema di Governance.

3.6.2 Specifiche per l'invio delle mail.

Le mail che saranno scambiate, tra il referente dell'Amministrazione e gli operatori del SOC, nella fase di richiesta della diversion e nelle fasi successive fino alla disattivazione della diversion avranno tutte un formato pre-definito che sarà concordato tra le parti nella fase di attivazioen del servizio.

In generale le mail che saranno scambiate tra il referente dell'Amministrazione ed il personale del SOC sono le seguenti:

- "Richiesta di attivazione della "diversion": è la mail con la quale il Cliente segnala un sospetto attacco DDoS. Il Cliente invierà questa mail sia allo SPOC che al SOC,
- "Referente non autorizzato": è la mail che il SOC invia al Cliente ed allo SPOC per segnalare che il richiedente non è tra gli utenti abilitati a richiedere l'attivazione della diversion.
- "Informativa attivazione servizio": è la mail che il SOC invia al Cliente ed allo SPOC per notificare l'avvenuta attivazione della diversion.
- "Cessato allarme": è la mail inviata dal SOC al referente Cliente per richiedere la disattivazioen della diverson inquanto l'attacco DDoS è sttao risolto.
- "Richiesta disabilitazioen diversion": è la mail di risposta alla mail del punto sopra da parte del referente Cliente che autorizza a riportate il traffico sul percorso normale.
- "Conferma disabilitazione diversion": è la mail inviata dal SOC al referente cliente per avvisarlo che il traffico è sttao riportato sul percorso normale.

3.6.3 Descrizione delle fasi per gestione attacco DDoS.

Nel seguito vengono dettagliate le diverse fasi relative alla gestione di un attacco DDoS.

Richiesta attivazione "diversion"

A seguito di sospetto attacco DDoS il refernte dell'Amministrazione contetterà telefoncamente lo SPOC o aprirà un pre-ticke sul sistema di TTM di SPC e contestualmente invierà una mail di di "Richiesta di attivazione diversion" sia allo SPOC che al SOC.

La mail di "Richiesta di attivazione diversion" dovrà contenere le seguenti informazioni:

- Elenco degli indirizzi IP/32 target che devono essere oggetto dell'azione di mitigation,
- tutti i servizi eventualmente esposti dagli IP indicati al fine di poter ottimizzare i filtri imposti per la mitigation.

Il SOC, una volta ingaggiato dallo SPOC, potrà contattare il Cliente per avere ulteriori informazioni.

Attivazione servizio

L'operatore del SOC, dopo avere eseguito le opportune analisi, attiva manualmente la protezione degli indirizzi IP interessati e procede con le azioni di contenimento.

L'operatore del SOC, notifica, tramite mail al referente Cliente e allo SPOC, l'avvenuta attivazione della diversion; lo SPOC provvede a chiudere il ticket sul sistema SPC.

Analisi dell'attività e/o contenimento dell'attacco

L'operatore del SOC procede con le azioni di contenimento e trascorso un tempo ritenuto congruo ai fini dell'analisi in corso aggiorna, telefonicamente e/o inviando una mail il referente Cliente che ha avviato la richiesta, sull'andamento dell'attacco in corso e\o sull'analisi effettuata.

Cessato allarme

Non appena l'operatore del SOC accerta che si siano verificati uno o più dei seguenti casi:

- il traffico malevolo è sceso al di sotto della soglia d'attenzione;
- gli strumenti di controllo danno evidenza della conclusione dell'attacco DDoS;

contatta telefonicamente il referente dell'Amministrazione che ha avviato la richiesta riguardo la possibilità della disattivazione della Diversion precedentemente attivata e contestualmente invia una mail (mail "Informativa cessato allarme") di richiesta disattivazione Diversion..

Conferma di cessato allarme

In risposta all'avviso di cessato allarme, comunicato dall'operatore del SOC, il referente Cliente che ha avviato la richiesta, invia una mail (mail "Richiesta disabilitazione del servizio DDoS Mitigation"), nella quale autorizza esplicitamente l'eliminazione della "Diversion" del traffico ed il ripristino della normale modalità operativa.

Qualora non vi sia conferma esplicita oppure il referente Cliente dichiari espressamente di non autorizzare la disattivazione della "Diversion", l'operatore del SOC dovrà inviare all'Amministrazione una mail (mail di "Responsabilità di mancata disattivazione del servizio DDoS Mitigation") in cui si notifica l'esplicita richiesta di mancata disattivazione della diversion da parte del referente Cliente.

Informativa disattivazione del servizio

Ricevuta via mail (mail “Richiesta di disattivazione del servizio DDoS Mitigation”) la conferma da parte del referente che ha avviato la richiesta, l’operatore del SOC, procede al ripristino della normale modalità operativa inviando una e-mail (mail “Conferma disabilitazione del servizio DDoS Mitigation”).

Incident Report

Il personale del SOC produce un ”Incident Report” in cui sono riportate le informazioni relative all’attacco e lo invia ai referenti Cliente che sono stati definiti in fase di implementazione del servizio.

L’Incident Report sarà inviato, tramite mail con opportuno template (mail “Incident Report”), in formato .zip con password. La password e verrà comunicata telefonicamente contattando un NV con PIN che sarà comunicato al Cliente.

L’Incident Report sarà prodotto dal SOC entro due giorni lavorativi dal termine del servizio di DDoS Mitigation.