Gestione degli Incidenti di Sicurezza sulla rete GARR

Premesse

Riferimenti per gli incidenti di sicurezza

Ogni entità collegata alla rete GARR deve nominare il proprio responsabile tecnico locale, l'APM (Access Port Manager). L'APM gestisce il collegamento con la rete GARR ed è la persona di riferimento tecnico presso il GARR per la sua istituzione anche per quanto riguarda la gestione degli incidenti di sicurezza. La definizione di APM è disponibile sul sito istituzionale GARR. [https://www.garr.it/it/comunita/la-comunita-garr/gli-apm].

Comunicazioni

Le comunicazioni emesse dal GARR-CERT verso i soggetti coinvolti si svolgono principalmente tramite posta elettronica, con firma PGP (cert.garr.it/it/pgp/garr-cert-pgp-keys).

Protezione da attacchi esterni distribuiti

Da ottobre 2019, la rete GARR è dotata di un sistema automatico per la mitigazione di alcune tipologie di attacchi esterni, distribuiti e mirati a creare disservizi (DDoS - Distributed Denial of Service), basato su tecnologia Corero|Juniper (www.corero.com). Quando alcuni indicatori superano i valori di soglia, gli apparati di rete reagiscono ed eliminano selettivamente il traffico corrispondente a questo tipo di attacchi applicando dei filtri temporanei, permettendo così ai singoli nodi di mantenere normale funzionalità della rete. La procedura avviene in maniera automatica, senza nessun intervento da parte degli utenti. L'individuazione degli indicatori da utilizzare e i rispettivi valori di soglia sono configurati dal GARR-NOC.

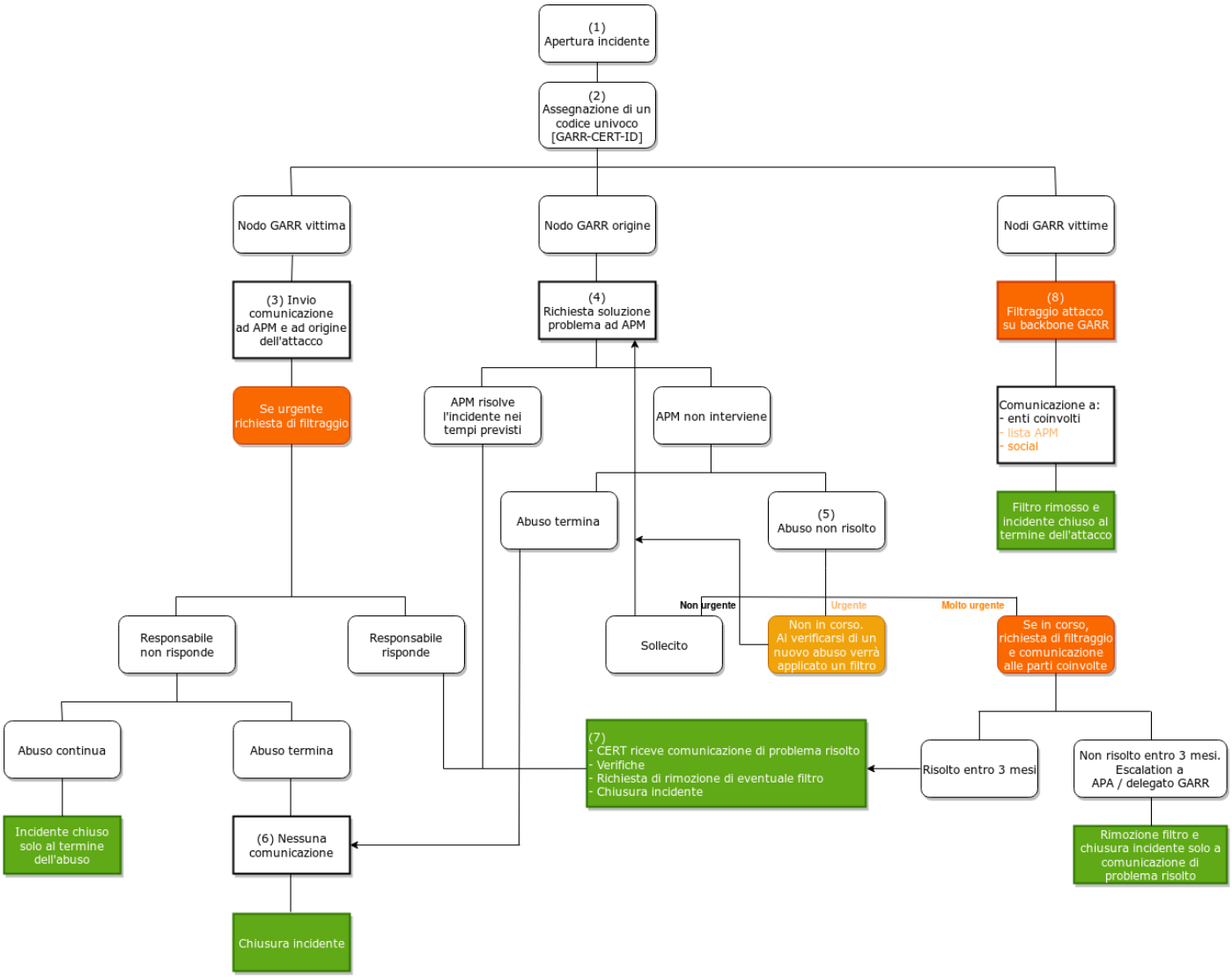
Filtraggio

La gestione incidenti prevede, in alcuni casi particolari, il filtraggio di uno o più indirizzi di rete sulle interfacce dei router gestiti da GARR.

Ci preme sottolineare che l'applicazione di tali filtri è sempre da intendersi a protezione e salvaguardia della funzionalità della rete e dei servizi di connettività a disposizione degli utenti della rete GARR. Nel caso più evidente in cui gli IP GARR sono i bersagli diretti o indiretti di eventuali attacchi esterni, spesso sono gli stessi utenti (APM) a chiedere l'intervento del filtraggio al CERT/NOC per recuperare l'accesso ai loro dispositivi di frontiera e possibilmente intervenire sulle loro configurazioni per mitigare anche localmente il problema.

Nel caso in cui gli IP GARR siano sorgenti di traffico palesemente illecito e non vi sia alcuna risposta da parte dell'APM nei tempi previsti, gli IP coinvolti vengono filtrati da GARR (con i criteri descritti nella procedura di gestione degli incidenti di sicurezza), allo scopo di tutelare i propri utenti e prevenire da eventuali conseguenze legali. Dopo tre mesi dall'avvenuto filtraggio, in assenza di risposta da parte dell'APM, si procederà ad informare l'APA e il Delegato GARR dell'Ente di competenza (escalation).

Flusso della Procedura di Gestione Incidenti



Procedura di gestione incidenti adottata da GARR-CERT

1) Al verificarsi di un problema di sicurezza che veda coinvolto un soggetto appartenente alla rete GARR, GARR-CERT valuta l'apertura di un incidente di sicurezza e ne decide la priorità, le procedure di risoluzione e le modalità di comunicazione con i soggetti coinvolti.

2) GARR-CERT assegna all'incidente un codice univoco (Ticket ID).

- Nel caso in cui il soggetto GARR sia vittima dell'evento illecito, segue al punto 3.
- Nel caso in cui il soggetto GARR sia origine dell'evento illecito, segue al punto 4.
- Nel caso in cui l'evento illecito provenga da una o più sorgenti e sia destinato contro più utenti GARR, segue al punto 8.

3) GARR-CERT invia all'APM una comunicazione informativa e ai contatti opportuni per il sistema origine dell'abuso.
In casi di particolare gravità ed urgenza, GARR-CERT valuta se richiedere un filtraggio temporaneo al GARR-NOC per mitigare l'attacco, quando non già applicato dal sistema di mitigazione automatica di DoS.

- Se l'abuso termina e il riferimento per il sistema che lo ha originato non risponde, segue al punto 6.
- Se il riferimento per il sistema che ha originato l'abuso risponde, segue al punto 7.
- L'incidente viene chiuso solo al termine dell'abuso.

4) GARR-CERT chiede all'APM di risolvere l'incidente entro un tempo commisurato alla gravità del caso (in calce alcuni esempi di tempistiche per tipologia di abuso). Quando possibile, fornisce anche indicazioni e suggerimenti utili. Se ritenuto opportuno, GARR-CERT risponde anche a coloro che hanno segnalato l'incidente.

- Nel caso in cui l'APM intervenga entro i tempi richiesti, segue al punto 7.
- Nel caso in cui l'APM non intervenga entro i tempi richiesti e l'abuso cessi, segue al punto 6.
- Nel caso in cui l'APM non intervenga entro i tempi richiesti e l'abuso continui, segue al punto 5.

5) GARR-CERT procede in uno dei seguenti modi, a seconda della gravità del caso:

- Invia una mail di sollecito (2a comunicazione, ecc.) all'APM, invitandolo nuovamente ad intervenire. Tornare al punto 4.
- Invia un avviso di filtraggio all'APM (e in copia al GARR-NOC e alla direzione GARR) nel quale è scritto che se l'evento illecito dovesse proseguire o ripresentarsi, il GARR-NOC provvederà ad applicare un filtraggio temporaneo opportuno, senza ulteriori preavvisi. Tornare al punto 4.

- Procede a richiedere l'applicazione di un filtro opportuno al GARR-NOC e, successivamente alla conferma di avvenuto filtraggio, avvisa l'APM e le altre parti coinvolte.
- Se entro tre mesi dall'applicazione del filtraggio l'APM interviene per risolvere il problema, segue al punto 7, altrimenti si procederà ad informare l'APA e il Delegato GARR dell'Ente di competenza; l'incidente quindi verrà chiuso e il relativo filtro rimosso solo in seguito alla comunicazione di avvenuta risoluzione.

6) GARR-CERT non riceve alcuna comunicazione: l'incidente viene chiuso d'ufficio.

7) GARR-CERT riceve la comunicazione di avvenuta risoluzione del problema e, quando tecnicamente possibile, procede alla verifica delle azioni intraprese prima di chiudere l'incidente ed avvisare tutte le parti coinvolte.
Nel caso in cui sia stato applicato un filtraggio da parte del NOC, il CERT ne richiede la rimozione e attende conferma prima di chiudere l'incidente.

8) Esaminato il tipo di attacco tramite gli strumenti di monitoraggio disponibili, CERT e NOC si coordinano per applicare un filtro sul backbone GARR. Viene inviata notifica ai contatti opportuni per la rete o le reti origine dell'abuso, agli utenti coinvolti, singolarmente o alla mailing list degli APM, ed eventualmente viene pubblicata la notizia seguendo i canali di comunicazione di GARR [web, social]. La chiusura dell'incidente e la rimozione dei filtri sul backbone sono subordinate alla verifica del termine dell'attacco.

Tipologia di incidenti trattati attualmente (con indicazione di tempistica d'intervento)

In funzione della tipologia, sono elencati i tempi richiesti per la risoluzione dell'incidente a partire dalla notifica. Nei casi in cui l'APM abbia bisogno di una dilazione dei tempi per risolvere l'incidente è necessario che ne faccia esplicita richiesta al GARR-CERT.

- Phishing (4 ore)
- DoS (5 ore)
- Connection Attempts (1 giorno)
- Compromised Node/Account (1 giorno)
- Probe (1 giorno)
- Malware/Virus (1 giorno)
- Vulnerable Node/Account (3 giorni)
- Spam (3 giorni)
- Piracy (3 giorni)

In caso di emergenza

Nel caso si verifichi un incidente, anche fuori dall'orario di attività di NOC e CERT, che impatti significativamente sulla connettività degli utenti, come per esempio un SYNFlood distribuito, i responsabili di NOC e CERT decidono le modalità di:

a) applicazione di eventuali filtri a livello di router GARR anche entro tempi inferiori a quelli previsti nella Procedura di Gestione Incidenti,

b) comunicazione agli utenti coinvolti e, sentito il Direttore del Dipartimento Network [e/o il Direttore del GARR], se e come diffondere l'evento e i dettagli ad altri soggetti o pubblicamente.

Anche altri casi che espongano gli utenti a gravi problemi di sicurezza, ad esempio nel caso di data breach in corso che riguardano dati particolari, possono essere trattati a scopo cautelativo come al precedente punto (a).

Riferimenti normativi

L'aggiornamento della Procedura di Gestione Incidenti di Sicurezza del GARR e' dovuta, oltre che all'evoluzione dei tipi di minacce sia esterne che interne alla rete e dei/ai sistemi degli utenti, anche all'evoluzione delle norme vigenti in Italia relative ai reati informatici.

Prima delle recenti direttive contenute nelle Misure Minime di Sicurezza per la Pubblica Amministrazione (AgID, 26/4/2016 - https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict) e del recepimento in Italia del Regolamento Europeo per la Protezione dei Dati Personali (D.lgs. 101/2018 - https://www.garanteprivacy.it/web/guest/provvedimenti/provvedimenti-a-carattere-generale), i reati informatici compaiono per la prima volta in Italia con la legge 547 del 1993, che introduce modificazioni e integrazioni del Codice Penale e del Codice di Procedura Penale in tema di criminalità informatica.

Questi sono, ad oggi, i reati informatici puniti dal Codice Penale:

- **Frode informatica** - Articolo 640 ter c.p. Consiste nell'alterare un sistema informatico per procurarsi un ingiusto profitto. Pena prevista: reclusione da sei mesi a tre anni e multa da 51 a 1.032 euro. Esempi: phishing.
- **Accesso abusivo ad un sistema informatico o telematico** - Articolo 615 ter c.p. Condotto da colui che si introduce in un sistema informatico o telematico protetto da misure di sicurezza, o vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo. Pena prevista: reclusione fino a tre anni. Secondo la giurisprudenza della Corte di Cassazione, commette il reato in esame colui che, pur essendo abilitato, acceda o si mantenga in un sistema informatico o telematico protetto, violando le condizioni ed i limiti risultanti dal complesso delle prescrizioni impartite dal titolare del sistema per delimitarne oggettivamente l'accesso.
- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici e telematici** - Articolo 615 quater c.p. Punita con la reclusione fino a un anno e con la multa fino a 5.164 euro. Reato commesso da chi - al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno - abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo.
- **Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico** - Articolo 615 quinquies c.p. Reclusione fino a due anni e multa sino a euro 10.329 per la diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico. Il reato è commesso da chi si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento.
- **Intercettazione, impedimento o interruzione illecita di comunicazioni** - Articoli 617 quater e 617 quinquies c.p. Viene sanzionato rispettivamente chi, senza essere autorizzato, intercetta, impedisce, interrompe o rivela comunicazioni informatiche e colui

che installa apparecchiature dirette ad intercettare, interrompere o impedire comunicazioni informatiche.

- **Falsificazione, alterazione, soppressione di comunicazioni e danneggiamento di sistemi** - Viene sanzionato dal codice penale anche chi falsifica, altera o sopprime la comunicazione informatica acquisita mediante l'intercettazione (articolo 617 sexies c.p.) e chi distrugge, deteriora, o cancella, dati, informazioni o programmi informatici (articolo 635 bis c.p.). E, con riguardo al reato di violazione e sottrazione di corrispondenza, la legge n. 547/1993, aggiornando l'articolo 616 c.p., precisa che per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza.