Scansioni di sicurezza e gestione degli incidenti su INFN CLOUD

Versione	Data	Commenti	Autori
1.0	2021 Gen 20	Prima versione	WP4
1.1	2021 Feb 18	Aggiunto hostname da dove provengono le scansioni. Rinominato “Security Team” in “Security Incident Team”. Aggiunto TOC e numeri di pagina	Massimo Sgaravatto
1.2	2021 Nov 26	Aggiunta la sezione relativa ai data breach	Massimo Sgaravatto

Contents

Il presente documento descrive le policy e le procedure attive su INFN Cloud per quel che riguarda le scansioni di sicurezza sugli host collegati in rete e la gestione degli incidenti di sicurezza.

Le figure coinvolte sono:

- INFN Cloud Security Incident Team
  - Il gruppo di lavoro che si occupa della sicurezza di INFN Cloud
- INFN CSIRT
  - Lo CSIRT dell’INFN

- Federated Site Administrator
    - Gli amministratori delle cloud federate
- System Administrator
    - Gli amministratori di istanze o servizi attivi sul backbone e sulle cloud federate

Scansioni di sicurezza

È un servizio offerto da INFN Cloud per il backbone e per le cloud federate. Il servizio esegue una scansione periodica degli IP pubblici attivi per mettere in evidenza quelle che possono essere eventuali vulnerabilità dei servizi esposti ad internet.
Il servizio è in esecuzione sul backbone di INFN Cloud, su una o più VM dedicate. L'hostname da dove provengono le scansioni è *scans.cloud.infn.it*.

Scansioni sui floating IP del backbone e sugli IP pubblici dei servizi core di INFN Cloud

Attraverso le API OpenStack si ottiene la lista dei floating IP (FIP) allocati. Accedendo al DNS si ottiene, per ogni IP, la lista di eventuali nomi associati, allo scopo di eseguire la scansione sugli hostname anziché sugli indirizzi IP. In questo modo migliora la rilevazione di vulnerabilità sui servizi basati su HTTP.
Le scansioni sui nomi associati ai FIP o direttamente sui FIP vengono eseguite periodicamente, almeno una volta alla settimana. Anche gli indirizzi IP pubblici associati ai servizi core di INFN Cloud, sia nel backbone che nei siti federati, sono soggetti a scansioni di sicurezza periodiche.

Scansioni sugli IP pubblici delle cloud federate

Per quanto riguarda le cloud federate, è necessario poter ottenere dinamicamente ed in maniera automatica la lista degli IP pubblici allocati dai progetti collegati ad INFN Cloud ed eventualmente i nomi DNS ad essi associati, se disponibili. Questo è possibile grazie ad un utente di servizio, presente sulle cloud federate, che può listare gli indirizzi IP pubblici utilizzati all'interno di ogni progetto legato ad INFN Cloud.
Anche in questo caso le scansioni vengono eseguite periodicamente, almeno una volta alla settimana.

Accesso interattivo alla piattaforma

L'accesso alla piattaforma di gestione delle scansioni, contenente le informazioni complete sui risultati delle stesse e dal quale è possibile, se necessario, lanciare scansioni al di fuori del normale programma periodico, è limitato ai membri dell'INFN Cloud Security Incident Team per una visione totale. Ai Federated Site Administrator sarà dato accesso ad una vista che interessa solo le risorse di cui sono responsabili.

Gestione degli incidenti

L'elevato grado di interconnessione tra le cloud federate richiede una gestione uniforme degli incidenti che si verificheranno. A questo scopo INFN Cloud centralizza questo servizio nel suo INFN Cloud Security Incident Team, secondo la procedura descritta più avanti. Tale

procedura dovrà essere seguita da tutte le cloud federate qualora venga scoperto un incidente di sicurezza. Indipendentemente da chi faccia la segnalazione iniziale, l'INFN Cloud Security Incident Team includerà sempre nelle sue risposte il Federated Cloud Administrator della cloud federata, oltre al System Administrator dei servizi coinvolti. Il mancato rispetto della procedura avrà conseguenze commisurate alla gravità del caso e in accordo con le linee guida che verranno definite internamente dal Security Team, ma che possono arrivare alla sospensione dalla federazione.

Procedure di gestione delle vulnerabilità rilevate

L'INFN CLOUD Security Incident Team potrebbe segnalare, o come risultato di una scansione, o come segnalazione dello CSIRT, la presenza di vulnerabilità nel software. La segnalazione includerà sempre, almeno in copia, il Federated Site Administrator della cloud federata, che sarà responsabile di verificare che la correzione della vulnerabilità avvenga secondo i tempi previsti. Anche in questo caso, la mancata correzione del problema avrà conseguenze che, a seconda della gravità, potrebbero arrivare alla sospensione della cloud federata.

Notifiche

Nel caso in cui venga rilevata una vulnerabilità, il System Administrator della VM associata all'indirizzo IP pubblico viene notificato con un e-mail.
Il messaggio deve specificare quali siano le vulnerabilità per le quali è richiesta un'azione, quali siano le azioni richieste, quali siano i tempi attesi per risolvere il problema, e le modalità per contattare l'INFN Cloud Security Incident Team in caso di necessità di supporto per la risoluzione del problema.
La notifica di cui sopra è inviata via e-mail anche al Security Incident Team di INFN Cloud e, nel caso l'indirizzo IP pubblico appartenga ad una Cloud federata, al Federated Site Administrator della cloud federata.
Nel caso invece la vulnerabilità riguardi un servizio core, in esecuzione sul backbone o su un sito federato, il problema viene riportato al relativo Federated Site Administrator. Anche in questo caso la notifica viene inviata in copia al Security Incident Team di INFN-Cloud.

Tempi di risposta e severità delle vulnerabilità

Le vulnerabilità vengono classificate in quattro categorie a secondo della loro gravità.

Gravità indicata dal CSIRT	**Vulnerabilità indicata dalle scansioni**	**Tempo Limite**
CRITICA	9, 10	Indicato nella segnalazione, ma <= 1 settimana
ALTA	6, 7, 8	6 settimane
MEDIA	4, 5	6 mesi
BASSA	1, 2, 3	8 mesi

Il system administrator che riceve la segnalazione può scegliere di non risolvere una

vulnerabilità indicata come bassa (o minore di 4, per quelle indicate dalle scansioni) ma deve documentare questa scelta e comunicarla nella risposta.

Se la vulnerabilità non viene risolta nei tempi indicati, la VM deve essere isolata e l'account del suo proprietario deve essere temporaneamente disabilitato. Questa procedura si applica al backbone ed alle risorse INFN-Cloud sulle cloud federate.
Spetta al Security Incident Team di INFN-Cloud il compito di notificare gli amministratori del backbone o del sito federato quando queste operazioni (di isolamento della istanza vulnerabile, e di banning dell'utente) devono essere fatte.

Se la vulnerabilità riguarda un servizio core di un sito federato, questa deve essere risolta (nei tempi sopra indicati) dal relativo Federated Site Administrator. Il Federated Site Administrator può contattare il Security Incident Team di INFN Cloud nel caso siano necessari chiarimenti o assistenza per la risoluzione del problema.
Se la vulnerabilità non viene risolta nei tempi previsti, il sito può essere sospeso, come riportato nelle Rules of Participation di INFN Cloud.

Procedure di gestione degli incidenti

La procedura di gestione degli incidenti è dettagliata nella seguente tabella:

Event or Action	Timing	Notes
Alla scoperta di un incidente di sicurezza, chi scopre l'incidente deve segnalare la cosa al Security Incident Team di INFN-Cloud. Quest'ultimo, una volta verificato che la segnalazione sia effettivamente un incidente, dovrà creare la segnalazione per INFN CSIRT inviando una e-mail all'indirizzo csirt@infn.it. Verrà aperto un ticket automaticamente che dovrà essere referenziato ad ogni successiva comunicazione con INFN CSIRT semplicemente rispondendo alla mail relativa al ticket in questione che avrà Oggetto (Subject) nel formato [INFN CSIRT #number] L'INFN Cloud Security Incident Team prenderà come contatti per le sue comunicazioni sia il System Administrator dei	Entro 4 ore dalla scoperta dell'incidente	La segnalazione dovrà contenere come minimo gli indirizzi IP dei nodi coinvolti, divisi tra vittime e attaccanti ed i riferimenti esatti di data e ora. Ulteriori dettagli sono graditi ma non necessari. Lo scopo di questa mail è di fornire un'iniziale segnalazione dell'incidente.

servizi interessati, sia il Federated Site Administrator. Nel caso si sospetti un data breach, l'INFN Cloud Security Team avviserà il Direttore della struttura INFN che ospita il sistema coinvolto.		
In collaborazione con il Security Incident Team di INFN Cloud e con lo CSIRT, il Federated Site Administrator dovrà isolare i sistemi coinvolti senza eliminare le informazioni necessarie per l'analisi forense	1 giorno lavorativo dalla scoperta dell'incidente	Se possibile, effettuare uno snapshot della macchina. Isolare la macchina a livello di rete dalle altre. NON fare reboot o spegnere la macchina. Se la macchina compromessa è una VM, non distruggere la VM. Se necessario, staccare fisicamente la macchina dalla rete. Il Security Incident Team di INFN Cloud rimane disponibile per consulenza e collaborazione.
In collaborazione con il Security Incident Team di INFN Cloud e con lo CSIRT, il Federated Site Administrator deve decidere se sono necessarie ulteriori analisi ed approfondimenti dell'incidente	1 giorno lavorativo dalla scoperta dell'incidente	A questo scopo, seguire la checklist CHECK1 di seguito per controllare quali informazioni dovrebbero essere raccolte. Se un'informazione è impossibile da recuperare o non si applica non è un problema, ma la cosa deve essere gi~~s~~ustificata. Se una qualunque delle altre informazioni è mancante, allora un'ulteriore analisi è necessaria. Una guida di base all'analisi forense si può trovare su https://analisi-forense.it
Se necessario, il Federated Site Administrator deve annunciare un downtime per i servizi coinvolti	1 giorno dall'isolamento iniziale	
Il Federated Site Administrator, unitamente, se necessario, ai System Administrator dei servizi coinvolti, deve effettuare	Iniziare subito dopo l'isolamento della macchina, continuare fino a quando non si è in grado di fornire un report completo secondo	Perché l'analisi sia completa, si dovrebbero avere tutte le informazioni presenti in CHECK1 che si è stati in grado di recuperare, escluse quelle

un'analisi dell'incidente di sicurezza.	CHECK1. In ogni caso, finire entro due settimane dalla segnalazione iniziale	possibilmente non rilevanti. Il Security Team di INFN Cloud collabora nell'attività di analisi forense. Qualora nel corso dell'analisi risultasse che l'attacco si è esteso anche ad altre macchine del sito, anche queste dovranno essere isolate fino a risoluzione ed occorrerà applicare anche ad esse la procedura corrente.
Alla chiusura dell'incidente, il Federated Site Administrator deve inviare un report definitivo citando le soluzioni adottate, rispondendo al ticket aperto dallo CSIRT e mettendo in copia il Security Team di INFN Cloud	Appena possibile, al massimo entro due settimane dalla chiusura	La chiusura avviene quando l'incidente è stato compreso, e quando si sia ragionevolmente certi che non vi siano più tracce dell'attaccante nel sistema, e che il metodo usato per l'attacco non sia più praticabile.