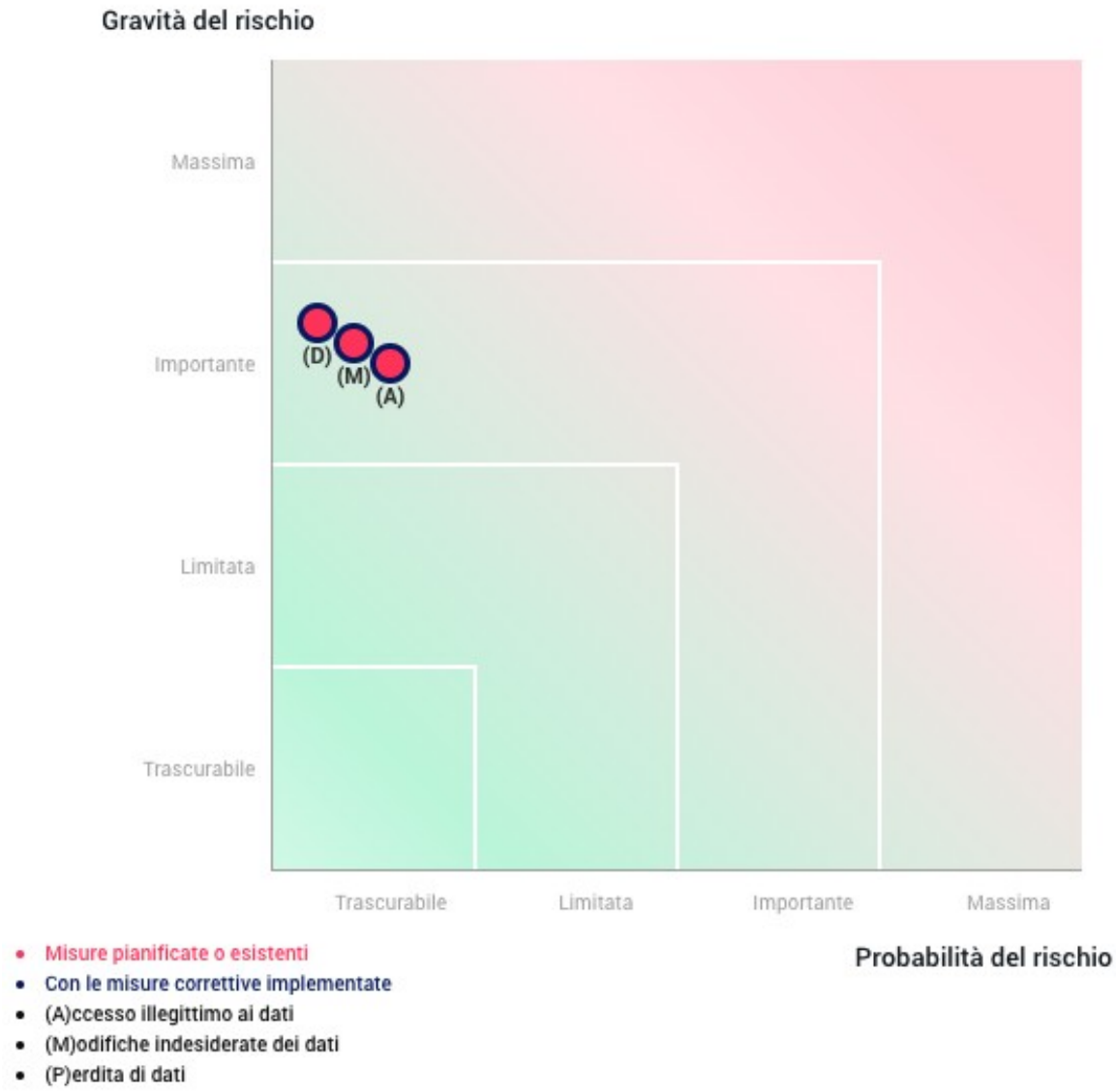
CERT-Ransomfeed

Editing :
Fadda Dario
Evaluation :
Fadda Dario
Validation :
Fadda Dario
Status :
Validata
100%

Validation

Mappa dei rischi



Validation

Piano d'azione

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

Validation

DPO and data subjects opinion

Nome del DPO/RPD

Dario Fadda

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

L'aumento degli attacchi cibernetici al settore delle PMI italiane, guardando l'andamento degli ultimi tre anni non accenna a diminuire. Dotare le aziende attualmente sprovviste di una misura di questo tipo è un grande passo avanti nella propria resilienza informatica.

Richiesta del parere degli interessati

È stato chiesto il parere degli interessati.

Nomi degli interessati

PMI italiane

Posizione degli interessati

Il trattamento può essere implementato.

Pareri degli interessati

E' stato intervistato un campione di aziende colpite da attacco di tipo ransomware nell'anno 2024, hanno dato parere favorevole all'installazione dell'Agent per una migliore sicurezza delle proprie macchine, riconoscendone i benefici.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

CERT-Ransomfeed si prefigge di creare una rete di PMI italiane che possano adottare misure di sicurezza avanzate rispetto alle attuali, al fine di migliorare la propria resilienza cibernetica alle minacce. Operare un monitoraggio automatico delle macchine che si vuole proteggere, con l'installazione dell'Agent software che lavora in perfetta simbiosi con qualsiasi antivirus, senza ostacolarne il lavoro ma arricchendone le attività di indagine. Il risultato finale è quello di poter allertare la singola azienda via email, al verificarsi di un evento malevolo o potenziale sospetto, dando così la possibilità di intervenire prima che lo scenario esploda in minaccia.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento è responsabile del funzionamento dell'Agent software, degli indirizzi email che vengono richiesti al fine di poter indirizzare gli alert e della conservazione dei log tecnici che vengono analizzati dalla piattaforma connessa all'Agent, di proprietà esclusiva di CERT-Ransomfeed, senza alcun utilizzo di piattaforme in cloud presso terzi.

Ci sono standard applicabili al trattamento?

La piattaforma core del CERT-Ransomfeed è Wazuh. Tale sistema è compliance relativamente al trattamento dei dati secondo gli standard imposti dai framework PCI DSS, HIPAA, NIST 800-53, TSC e GDPR.

Valutazione : Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Il dato trattato per ogni azienda aderente al servizio è l'indirizzo email richiesto per poter recapitare gli alert in caso di sospetta minaccia (la cui conservazione è a revoca da parte dell'azienda: con la disinstallazione di tutti gli Agent relativi alla stessa azienda, si ottiene l'immediata cancellazione dell'indirizzo email da tutti i sistemi di CERT-Ransomfeed.

I dati trattati per ogni macchina su cui si decide di installare l'Agent software sono i seguenti:

- Identificativi dei sistemi e degli utenti (hostname, nomi utente di dominio).

- Indirizzi IP pubblici e privati.
- Eventuali file path o metadati associati a file/processi malevoli (in nessun caso vengono esfiltrati file dalla macchina che ospita l'Agent).
- Eventi di rete (tentativi di accesso, traffico sospetto).
- Dati tecnici relativi alla sicurezza (hash di file, certificati SSL, logon falliti e chiavi di registro Windows).

Non vengono trattati dati sensibili o giudiziari.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il trattamento dei dati a responsabilità del CERT-Ransomfeed inizia con la procedura di enrollment esposta sul sito (https://cert.ransomfeed.it).
La prima fase riguarda l'installazione dell'Agent sulla propria macchina aziendale.

- Da questo momento in poi l'Agent inizia la raccolta e l'analisi costante dei dati da esso trattati, in tempo reale mentre la macchina è accesa e collegata alla rete Internet.
- L'archiviazione dei dati trattati dall'Agent software viene operata su una macchina dedicata unicamente a questo scopo, di proprietà di CERT-Ransomfeed (nella persona di Dario Fadda).
- La conservazione dei dati è operata per 20 giorni, dopo tale tempo la piattaforma Wazuh ne certifica la cancellazione permanente dal server.
- Quando una azienda disinstalla tutti gli Agent dalle proprie macchine, i dati relativi a queste macchine e l'indirizzo email della società precedentemente raccolto, vengono eliminati entro le 24 ore.

Quali sono le risorse di supporto ai dati?

I supporti all'erogazione delle finalità di CERT-Ransomfeed sono:

- la piattaforma Wazuh, installata standalone senza lo sfruttamento di servizi condivisi o erogati da terzi (Wazuh Inc. inclusa);
- il sistema operativo GNU/Linux del server che ospita la piattaforma;
- ma macchina server fisicamente localizzata nel datacenter della società DigitalOcean LLC nella città di New York (USA).

Il CERT-Ransomfeed si compone anche di altri asset utili allo svolgimento delle proprie attività di cybersecurity ma che non hanno alcun legame con il servizio che viene offerto alle aziende, che per trasparenza vengono comunque esplicitati:

- seconda macchina server dedicata, fisicamente localizzata presso il datacenter di Oracle Cloud Infrastructure, adoperata per lavorazioni interne di Cyber Threat Intelligence.
- terza macchina server VirtualMachine, fisicamente localizzata presso il datacenter di Hostinger nei Paesi Bassi, adoperata per la pubblicazione del sito Internet pubblico (https://cert.ransomfeed.it)

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

L'unica finalità della raccolta dei dati trattati (email aziendale e operatività dell'Agent) è quella di poter rilevare in tempo reale un sospetto di minaccia cibernetica (utilizzo malevolo della macchina aziendale con potenziale rischio per la tenuta informatica dell'azienda), allertare il contatto indicando. Fornendo così tutti gli indicatori utili a interrompere lo scenario della minaccia.
Nessun accesso diretto ai contenuti (e alle macchine) dei dati aziendali viene operato da parte di CERT-Ransomfeed.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi giuridiche che rendono lecito il trattamento sono il "Consenso informato delle PMI aderenti", pubblicamente esposto sul sito di CERT-Ransomfeed (https://cert.ransomfeed.it) e "l'interesse legittimo alla protezione dei sistemi informativi" dell'azienda stessa.
Il consenso informato viene anche inviato direttamente alla email dell'azienda per la presa visione, ad ogni fase di enrollment nuova macchina.

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

CERT-Ransomfeed ha scelto di utilizzare la piattaforma Wazuh per il servizio offerto, per poter operare un trattamento dei dati il più possibile minimizzato rispetto alle finalità.
Si tratta della tipologia di dati (i log di sistema) minima necessaria per eseguire analisi di cybersecurity in grado di far scattare un alert in caso di minaccia.
Le informazioni trattate sono strettamente necessarie per il monitoraggio della sicurezza e la segnalazione degli incidenti.
Sono raccolti solo dati tecnici utili a identificare attività anomale o dannose.
Nessuna azienda o ente terzo diverso da CERT-Ransomfeed (nella persona di Dario Fadda) è autorizzato all'accesso a tali dati.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati raccolti non vengono manipolati in alcun modo dalla piattaforma, ma unicamente archiviati per l'analisi. Le regole che fanno scattare gli alert a seguito di minaccia sono costantemente aggiornate mediante confronto con IoC raccolti dalla fonte di settore VirusTotal.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

La conservazione dell'indirizzo email dell'azienda aderente, per un tempo illimitato fino a revoca (disinstallazione totale di tutti gli Agent afferenti ad essa) o altra espressa richiesta, è necessaria per poter recapitare gli alert che vengono generati tempo per tempo.
La conservazione stabilita in 20 giorni dei log acquisiti, è minimizzata il più possibile per aderire al regolamento GDPR, necessaria ad avere tutto il materiale indispensabile da fornire alle società aderenti, per indagare un incidente di sicurezza e portarlo alla chiusura. Questo in ottica di ricerca nei giorni successivi all'incidente, per otemperare a richieste eventualmente fatte alle società, da organismi di vigilanza e controllo in sede di audit.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

La presente informativa così come il modulo di "Consenso informato" vengono resi disponibili pubblicamente agli interessati sul sito Internet di CERT-Ransomfeed (https://cert.ransomfeed.it) e in tutti i casi di richieste specifiche mediante posta elettronica scrivendo a cert@ransomfeed.it

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Come espressamente indicato durante le fasi di enrollment, il Consenso Informato si considera visionato e accettato durante lo step di esecuzione del comando di avvio dell'Agent. Viene altresì trasmesso alla prima comunicazione di dati email della società che sta eseguendo l'enrollment.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Le richieste possono essere trasmesse a: cert@ransomfeed.it

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Le richieste possono essere trasmesse a: cert@ransomfeed.it

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Le richieste possono essere trasmesse a: cert@ransomfeed.it

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

L'unico responsabile del trattamento è Dario Fadda, che agisce per le finalità di CERT-Ransomfeed, operando con il ruolo di owner della piattaforma.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

L'Agent comunica con il server CERT-Ransomfeed con una connessione stabilita durante la fase di enrollment, questa comunicazione è crittografata utilizzando AES, con 128 bit per blocco e chiavi a 256 bit.

Anche le comunicazioni che avvengono all'interno del server tra l'analizzatore degli eventi e l'indexer, sono effettuate con crittografia TLS. Quest'ultima comunicazione è operata mediante lo strumento Filebeat.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Sicurezza dei canali informatici

Firewall dedicati e sistemi IDS/IPS

Valutazione : Accettabile

Controllo degli accessi logici

Autenticazione *forte* per l'accesso all'infrastruttura con doppio fattore (2FA).

Valutazione : Accettabile

Sicurezza dei siti web

Il sito pubblico è ospitato su macchine fisicamente separate da quelle che forniscono il servizio operativo per le finalità di CERT-Ransomfeed. Comunicazione cifrata TLS attiva durante la navigazione e fase di

enrollment.

Valutazione : Accettabile

Crittografia

I dati vengono cifrati utilizzando AES a 128 bit con chiave a 256 bit e TLS per le comunicazioni tra i componenti interni della piattaforma.

Valutazione : Accettabile

Backup

Sono implementati i backup sicuri della macchina server con snapshot giornalieri, su struttura esterna al server ma del medesimo datacenter di DigitalOcean LLC in New York, USA.
Questo sistema garantisce la regolare operatività con un immediato ripristino in caso di incidente all'infrastruttura di CERT-Ransomfeed.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Impatto alto, Perdita indirizzi email, Perdita log tecnici di sistema di aziende terze

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Furto autenticazione (2FA) dell'owner di CERT-Ransomfeed

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Sicurezza dei canali informatici, Crittografia

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, La gravità è Alta perchè sono dati riguardanti aziende terze che possono essere sfruttati per attacchi mirati.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, La probabilità è Bassa viste le misure messe in atto e l'inesistenza di personale interno oltre il responsabile del trattamento.

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Alert non attentibili, Mancata segnalazione incidenti gravi, Segnalazione di incidenti mai avvenuti

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Furto autenticazione (2FA) dell'owner di CERT-Ransomfeed

Quali sono le fonti di rischio?

Fonti umane esterne, Fonti umane interne

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Sicurezza dei canali informatici, Controllo degli accessi logici, Crittografia

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, L'impatto è Alto vista l'importanza dei dati trattati per il corretto funzionamento della piattaforma nei confronti di chi la utilizza per la propria sicurezza.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Trascurabile, La crittografia e il controllo degli accessi all'infrastruttura garantiscono una Bassa probabilità di verificare tale rischio.

Valutazione : Accettabile

Rischi

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita indirizzi email, Perdita log tecnici di sistema di aziende terze

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Furto autenticazione (2FA) dell'owner di CERT-Ransomfeed

Quali sono le fonti di rischio?

Fonti umane esterne, Fonti umane interne

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, L'impatto è Alto perchè log tecnici e di sicurezza possono essere utilizzati per attacchi mirati nei confronti delle aziende aderenti al servizio.

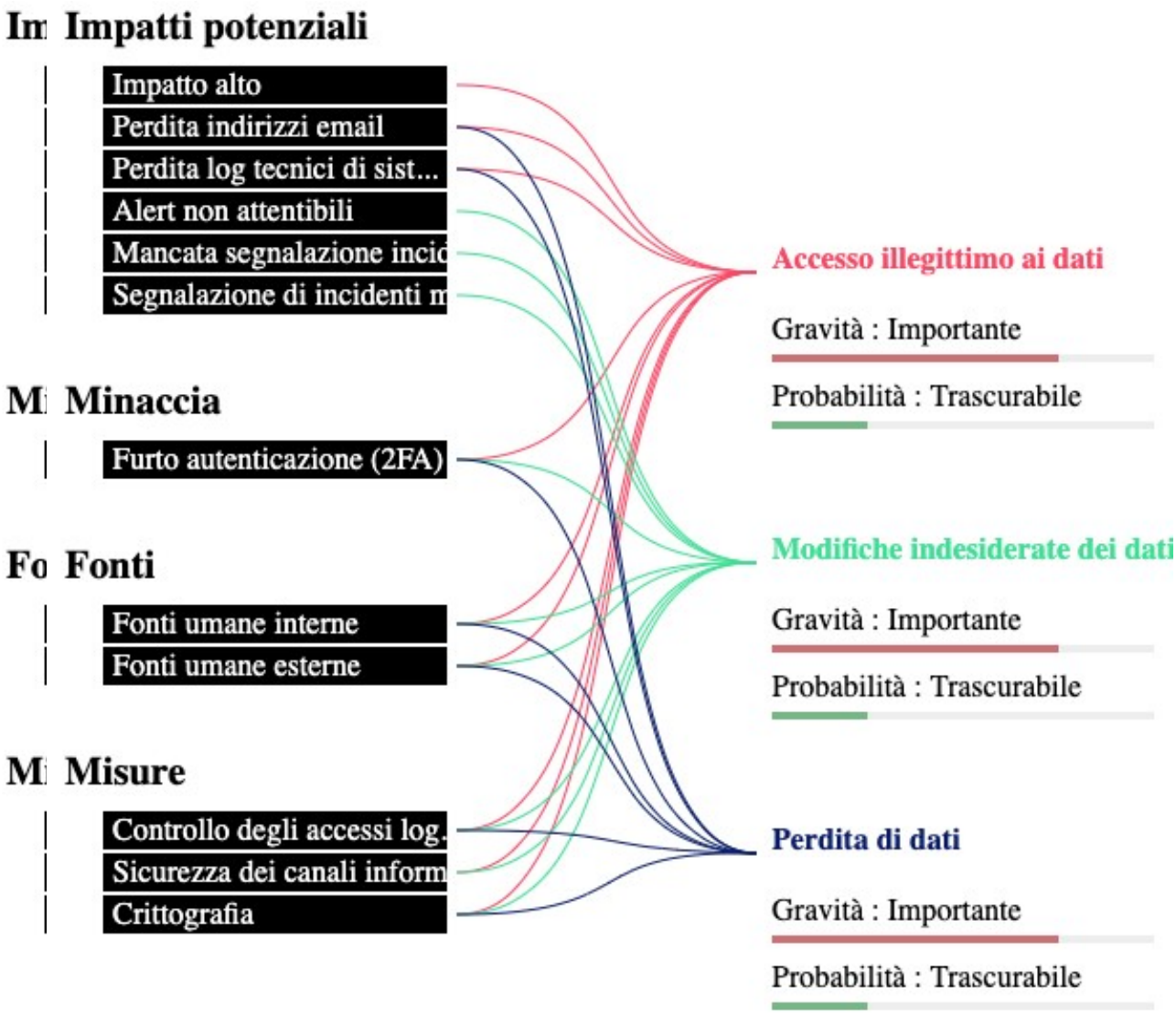
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Il furto dei dati operato senza un accesso autenticato all'infrastruttura non sarebbe utilizzabile grazie alla conservazione crittografata dei dati raccolti.

Valutazione : Accettabile

Rischi

Panoramica dei rischi


Im Impatti potenziali
Impatto alto
Perdita indirizzi email
Perdita log tecnici di sist...
Alert non attentibili
Mancata segnalazione inci
Segnalazione di incidenti n
M Minaccia
Furto autenticazione (2FA)
Fo Fonti
Fonti umane interne
Fonti umane esterne
M Misure
Controllo degli accessi log.
Sicurezza dei canali inform
Crittografia
Accesso illegittimo ai dati
Gravità : Importante
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Importante
Probabilità : Trascurabile
Perdita di dati
Gravità : Importante
Probabilità : Trascurabile