Workshop di CCR
24 - 28 maggio 2021

May, 24 2021

"Efficacia Probatoria dei file di log"

Vincenzo Ciaschini – CNAF
Nadina Foggetti – INFN Bari
Vincenzo Spinoso – INFN Bari

Indice

Applicazione del GDPR

1. Art. 24 par. 1 GDPR
2. Art. 32 GDPR
3. Art. 33 GDPR

- Principio di Accountability
- Obbligo per il titolare e il responsabile del trattamento il compito di individuare, implementare ed aggiornare un sistema di misure di sicurezza tecniche ed organizzative idonee a proteggere i dati personali da potenziali rischi quali la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso, accidentale o illegale, ai dati personali.
- Notifica dell'avvenuta violazione dei dati personali all'Autorità Garante per la Protezione dei dati personali, entro le 72 ore successive al momento della conoscenza della violazione stessa

Digital Evidence

1 Dir. 2016/1148

2 D.Lgs. 65/2018

- Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi, è stata recepita nel nostro ordinamento attraverso il decreto legislativo 18 maggio 2018, n. 65 (anche detto “decreto legislativo NIS”), in vigore dal 24 giugno 2018.
- Cyber crimes
- Eventuali danni causati da cui discenda una responsabilità civile
- Controversie in materia di diritto del lavoro

Il log ... come documento informatico

1. Art. 2712 CC
2. art. 20 DL 82/2005
3. Art. 2702 CC

- “le riproduzioni informatiche fanno piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime”
- “Codice Amministrazione Digitale”: il giudice civile ha facoltà di valutare il valore probatorio del documento informatico, tenendo conto delle caratteristiche di sicurezza, integrità e immodificabilità del documento medesimo.
- DPCM 13 novembre 2014, art. 3 comma 9.
- art. 2702 del Codice civile: “fa piena prova della provenienza delle dichiarazioni da chi l’ha sottoscritta”

Elementi essenziali:

- Integrità: «quella proprietà per effetto della quale si escludono alterazioni indebite delle tracce informatiche intervenute in epoca successiva alla creazione, trasmissione o allocazione in un supporto autorizzato”
- Catena di custodia: operazioni effettuate .
    - un sistema per mantenere e documentare, nel dettaglio, la raccolta, la gestione e preservazione della prova, insieme ad un record di chiunque sia venuto a contatta con la stessa.
    - Deve dimostrare che la prova è stata raccolta dal sistema in questione e che stata immagazzinata e gestita senza alterazioni.
- Non ripudiabilità : firma digitale e marcatura temporale

Log ... nella digital Forensic

1. CONVENZIONE BUTAPEST
2. ART. 491 BIS CP
3. ART. 247 C.P.P.

- Mancanza di standard universalmente riconosciuti
- Convenzione di Budapest sul cyber crime ha condotto alla modifica del concetto di documento informatico nell'ambito del codice penale
  - Introduce la possibilità di cristallizzare le prove acquisite adottato tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.
  - "quando si stratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità"
  - (art. 260 c.p.p.) ... quando la custodia (dopo l'acquisizione) riguarda dati informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi.

La giurisprudenza

1 Tribunale di Napoli 29704/2014 ordinanza

- I log possono essere considerati digital evidence, qualora gli stessi siano immodificabili e attendibili, ovvero al fine di produrre log efficaci quali prova processuale gli stessi devono essere firmati digitalmente e marcati temporalmente.
  - La giurisprudenza in materia ha ritenuto non ammissibili nel corso del processo le copie dei log, in quanto “le copie degli stessi non sono state estratte con modalità tali da garantirne, in caso di contestazione, la attendibilità e provenienza e la immodificabilità, né cristallizzati giuridicamente e processualmente in altro modo.

REQUIREMENTS:

1 INTEGRITA'

1 NON RIPUDIABILITA'

1 IMMODIFICABILITA'

- Integrità (strettamente connesse al sistema di cristallizzazione e conservazione dei log)
  - Definizione della catena di custodia: operazioni effettuate nel dettaglio.
  - Convenzione di Budapest : la copia deve esse conforme all'originale e la custodia deve essere tale da impedire l'alterazione e o l'accesso da parte di terzi.
- Non ripudiabilità dell'elemento raccolto: connessa a sistemi di autenticazione es. firma digitale e/o sistemi di marcatura temporale.
- Immodificabile (art. 20 CAD)
- Sistemi di conservazione e modalità tali da garantirne, in caso di contestazione, la attendibilità e provenienza e la immodificabilità. Ord. 29704/2014

Strategia Implementativa/1

interscambio tra sedi INFN

PRO

- Log al di fuori del controllo dell'admin delle sezione proprietaria
- Non si danno informazioni sensibili dell'INFN al di fuori dell'ente

CONTRO

- Terzietà quantomeno dubbia
- Si spostano gli obblighi verso i colleghi CHE DEVONO GARANTIRE:
  - che vengano conservati almeno per X tempo
  - che non siano stati modificati dal momento della consegna

Strategia Implementativa/2

Si consegnano i log ad un ente terzo che ne conserva e garantisce l'immutabilità

PRO

- Terzietà garantita

CONTRO

- Si danno informazioni (potenzialmente) sensibili al di fuori dell'ente
- Costi tutti da indagare
- Interfaccia? Scriptabile? Sito web? Applicazione dedicata?

Strategia Implementativa/3

•Si fa un .tar.gz dei log, se ne calcola l'hash, e si ottiene su di esso una marca temporale

PRO

- Non si distribuiscono log dell'INFN al di fuori dell'ente
- Costi ridotti (>90 euro + iva all'anno per sezione)
- Terzietà potenzialmente irrilevante

CONTRO

- Rimane il problema della conservazione dei log
- Da capire l'interfaccia: API? Web? App?

Strategia Implementativa/4

Acquisto di hardware dedicato

PRO

- Soluzione tutto in uno
- Solitamente hanno certificazioni che garantiscono l'efficacia (standard ISO 14721- OAIS.)

CONTRO

- Costi
- Lock-in

ParER - Polo archivistico dell'Emilia-Romagna

- Strumento già adottato dall'INFN (almeno) per l'archiviazione di protocollo, della documentazione di gara e per gli acquisti
- Specifiche tecniche note () https://poloarchivistico.regione.emilia-romagna.it/documentazione
  - informazioni preliminari acquisite da Claudio Ciamei (grazie!)
- Il versamento periodico del pacchetto di versamento previsto contenente metadati e log, dal punto di vista tecnico, è ampiamente implementato (N log file giornalieri, archiviazione)
- Il modello da utilizzare (XML) per i log è già disponibile: i metadati associabili alla singola richiesta di conservazione prevedono tutti i campi richiesti ai sensi del DPCM 13 novembre 2014, art. 3 comma 9, in particolare identificativo univoco e persistente, il riferimento temporale e l'impronta del documento
- L'INFN utilizza un intermediario (MAW) per il protocollo, ma non sembra strettamente necessario nel nostro caso (da approfondire)
- Il modello più corretto, in termini di efficienza (aggregazione) e di forma (versamento diretto sul conservatore) prevedrebbe la scrittura diretta da parte di ciascuna singola sezione di un aggregato di log, una volta al giorno

Nella prospettiva futura … "Linee guida sulla formazione, gestione e conservazione dei documenti informatici" … 2022

- maggiore chiarezza nei **ruoli e nei rapporti tra Titolare dell'oggetto della conservazione, Responsabile della conservazione e conservatore nei casi di affidamento all'esterno**. .
- Conservazione: il richiamo diretto allo standard Uni 11386 –SinCRO, pur se nella sua versione non aggiornata.
- Nel provvedimento viene ribadito che il sistema di conservazione non deve limitarsi a conservare documenti singoli, ma ove utile e/o necessario, deve provvedere a **conservare anche aggregazioni documentali unitamente ai loro metadati e ai loro vincoli archivistici** (eventualmente espressi negli stessi metadati o anche nell'indice dei pacchetti di archiviazione). È interessante, soprattutto nei casi di migrazione ad altro conservatore, il riferimento non più solo ai fascicoli (correttamente integrato con le serie documentali), ma anche ad interi archivi.


Question
Time

Grazie

Vicenzo– Nadina –
Vincenzo