Il sistema Anci a supporto
della digitalizzazione
dei Comuni

DIPARTIMENTO
PER LA TRASFORMAZIONE
DIGITALE

anci

Finanziato
dall'Unione europea
NextGenerationEU

Gli obblighi di notifica di incidenti Legge n.90/2024

Riccardo Santini

Divisione Gestione Rischio Nazionale, Capacità Cyber e Collaborazioni,
Servizio Operazioni e gestione delle crisi cyber, ACN

Obiettivo della lezione

Identificare alcuni elementi chiave

- Chi sono i soggetti con obbligo di notifica;
- Come riconoscere un incidente da segnalare e notificare;
- Quali sono le tempistiche associate alla segnalazione e notifica;
- Quali sono le sanzioni per il mancato adempimento dell'obbligo di segnalazione e notifica;
- Il flusso della segnalazione e della notifica.

L'articolo 1 della legge n. 90/2024

L’articolo 1 della legge n. 90/2024 “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”, impone obblighi di notifica ai soggetti individuati al comma 1 del medesimo articolo.

I soggetti con obbligo di notifica

Pubbliche amministrazioni centrali individuate ai sensi dell'articolo 1, comma 3, della legge 31 dicembre 2009, n. 196;

- regioni;
- province autonome di Trento e di Bolzano;
- città metropolitane;
- comuni con popolazione superiore a 100.000 abitanti;
- comuni capoluoghi di regione;
- società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- aziende sanitarie locali.

I soggetti con obbligo di notifica: le società in house

Tra i medesimi soggetti ricadono le società in house dei soggetti precedentemente elencati che forniscono i seguenti servizi:

- servizi informatici;
- servizi di trasporto di cui al precedente elenco;
- servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, come definite ai sensi dell'articolo 2, punti 1), 2) e 3), della direttiva 91/271/CEE del Consiglio, del 21 maggio 1991;
- servizi di gestione dei rifiuti, come definita ai sensi dell'articolo 3, punto 9), della direttiva 2008/98/CE del Parlamento europeo e del Consiglio, del 19 novembre 2008.

Il soggetto deve segnalare e notificare qualunque incidente:

- avente **impatto** su **reti, sistemi informativi** e **servizi informatici**;
- riconducibile a una delle tipologie individuate nella **tassonomia (c.d. ICP-C)** di cui all'art. 1, comma 3-bis, del decreto l**egge 21 settembre 2019 n.105**, convertito con modificazioni dalla legge 18 novembre 2019, n.133.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Un incidente è da definirsi tale quando incide sulla protezione, disponibilità, accessibilità, integrità e riservatezza dei dati e sulla continuità operativa dei sistemi e delle infrastrutture.

Tempistiche segnalazione/notifica

L'articolo 1, comma 2 della Legge n.90/2024 stabilisce che:

- **Comunicazione obbligatoria**
- la **segnalazione** deve essere effettuata **senza ritardo** e comunque **entro 24 ore** dal momento in cui si viene a conoscenza dell'incidente a seguito delle evidenze comunque ottenute;
- la **notifica**, relazionata alla precedente segnalazione, deve essere effettuata **entro 72 or**e a decorrere dal medesimo momento e **rappresenta una comunicazione completa di tutti gli elementi informativi disponibili**.

Sanzioni per il mancato adempimento dell'obbligo di segnalazione e notifica

Nei casi di **reiterata inosservanza**, nell'arco di cinque anni, dell'obbligo di notifica è prevista:

- Sanzione amministrativa pecuniaria **da euro 25.000 a 125.000**.

La **violazione delle disposizioni** dell'Art.1 comma 1 della Legge n.90/2024 può costituire:

- Causa di **responsabilità disciplinare e amministrativo-contabile** per i funzionari e i dirigenti responsabili.

Il flusso di segnalazione e notifica

I soggetti **effettuano la segnalazione di incidente** attraverso il modulo on-line disponibile sul sito del **CSIRT Italia:** *https://www.csirt.gov.it/segnalazione*

Legge 20 giugno, n.90 Soggetti sottoposti alle disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici (Legge n.90/2024)

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Le fasi del flusso

La **successiva notifica dell'incidente** segue un flusso diviso **in quattro fasi.** Ogni fase include un insieme di attività **che possono essere effettuate dal soggetto segnalante**.

1 - Preparazione alla notifica

2 - Notifica al CSIRT Italia

3 - Gestione della notifica

4 - Chiusura dell'incidente

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Nella Fase 1 della preparazione della notifica:

- **raccolta delle evidenze** (es. IOC, evidenze, azioni di ripristino) relative all'incidente stesso;
- **identificazione dei sistemi impattati;**
- **autovalutazione dell'impatto** sui sistemi e sull'erogazione dei servizi di business;
- **definizione e pianificazione** di un **piano di rientro**.

Rientrano in tale fase le attività di preparazione della segnalazione dell'incidente, ove prevista.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Nella Fase 2 della notifica al CSIRT Italia:

Fornire le seguenti informazioni:

- **data e ora** di rilevamento dell'incidente;
- **asset impattati;**
- **vettori d'attacco**;
- **misure di rientro** intraprese e pianificate;
- **IOC;**
- **evidenze rilevanti** (es. sample di malware, ransom note).

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE
anci
Finanziato dall'Unione europea NextGenerationEU

Nella fase 3 della gestione della notifica e 4 della chiusura dell'incidente:

- Dopo aver ricevuto **la notifica** da parte del soggetto segnalante, **CSIRT Italia** compatibilmente con le risorse a disposizione e la criticità del soggetto segnalante **offrirà supporto, se del caso in loco, nelle operazioni di incident handling.**
- Una volta definite ed avviate le attività di ripristino, si procederà alla **chiusura dell'incidente.**

Sintesi sulla segnalazione e notifica: i soggetti e gli obblighi

SOGGETTI LEGGE N. 90/2024

Soggetti individuati dall'**art.1, comma 1 della Legge n. 90/2024** «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

COSA SEGNALARE E NOTIFICARE AL CSIRT ITALIA

L'**obbligo di segnalazione e successiva notifica** è previsto dall'art.1, comma 2 della Legge n. 90/2024 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

Qualunque **incidente riconducibile a una delle tipologie individuate nella tassonomia** di cui al comma 1, come stabilito dall'art.1, comma 2 della Legge n. 90/2024 «Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici».

PERCHÉ SEGNALARE E NOTIFICARE AL CSIRT ITALIA

Sintesi sulla segnalazione e notifica: l'incidente e il CSIRT

COME RICONOSCERE UN INCIDENTE

Un **incidente** è da definirsi tale quando incide sulla protezione, disponibilità, accessibilità, integrità e riservatezza dei dati e sulla continuità operativa dei sistemi e delle infrastrutture.

I TEMPI DA RISPETTARE

La segnalazione e notifica sono **obbligatorie**:

- Segnalazione entro 24 ore;
- Notifica successiva entro 72 ore.

COME EFFETTUARE UNA SEGNALAZIONE E SUCCESSIVA NOTIFICA AL CSIRT ITALIA

È possibile effettuare una segnalazione e successiva notifica attraverso il **modulo disponibile sul sito internet CSIRT Italia.**

COSA ASPETTARSI DA CSIRT ITALIA

A seguito della segnalazione sarà aperto un **canale di comunicazione diretto**, relazionato alla successiva notifica, tramite il quale il CSIRT Italia offrirà al soggetto **supporto** alle attività di **incident handling**.

DIPARTIMENTO PER LA TRASFORMAZIONE DIGITALE

Finanziato dall'Unione europea NextGenerationEU

Grazie

per la vostra attenzione

r.santini@acn.gov.it

Il Sistema Anci a supporto della digitalizzazione dei Comuni