$whois Lino Fornaro

- Senior Security Manager (24 years in infosec)
- Lead Auditor ISO/IEC 27001:13
- **O**SSTMM **P**ROFESSIONAL **S**ECURITY **T**ESTER (OPST) E **S**ECURITY **A**NALYST (OPSA)
- **ISECOM** Certified Trainer
- Certificato ICT Security Manager – registro AICQ Sicev
- Docente Master sulla Sicurezza (ICS) presso TILS - L'Aquila
- Relatore in conferenze di sensibilizzazione sul tema ICT Security
- Esperto Normativa Europea sulla Data Protection (GDPR)
- Esperto normative europee Cybersecurity
- Membro Comitato Tecnico Scientifico **CLUSIT**
- Membro Comitato Tecnico Scientifico AICQ Sicev "Uni 11506 Certificazioni informatiche"
- Già Membro sottocommissione **SC27** di **UNINFO**

EVOLUMIA
The cyber security company

Clusit
Associazione Italiana per la Sicurezza Informatica

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

LE LEVE DELLA NIS2 PER L'EFFICACIA

ART. 1 *(Oggetto)*

Il presente decreto stabilisce misure volte a garantire un livello elevato di sicurezza informatica in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione europea in modo da migliorare il funzionamento del mercato interno.

Governance e responsabilità del management	Gestione dei rischi
Continuità operativa	**Gestione degli incidenti**
Formazione e awareness	**Sicurezza della supply chain**

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Focus on

- Gestione del Rischio
- Misure di sicurezza
- Gestione e segnalazione degli incidenti

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Capo IV - Obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente

- **ART. 23** ***(Organi di amministrazione e direttivi)***
- **ART. 24** ***(Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica)***
- **ART. 25** ***(Obblighi in materia di notifica di incidente)***
- **ART. 26** ***(Notifica volontaria di informazioni pertinenti)***
- **ART. 31** ***(Proporzionalità e gradualità degli obblighi)***
- **ART. 32** ***(Previsioni settoriali specifiche)***

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

DEFINIZIONI

«**rischio**»: la combinazione dell'entità dell'impatto di un incidente, in termini di danno o di perturbazione, e della probabilità che quest'ultimo si verifichi;

«**approccio multi-rischio**»: cosiddetto approccio *all-hazards*, l'approccio alla gestione dei rischi che considera quelli derivanti da tutte le tipologie di minaccia ai sistemi informativi e di rete nonché al loro contesto fisico, quali furti, incendi, inondazioni, interruzioni, anche parziali, delle telecomunicazioni e della corrente elettrica, e in generale accessi fisici non autorizzati;

DEFINIZIONI

«**sicurezza dei sistemi informativi e di rete**»: la capacità dei sistemi informativi e di rete di resistere, con un determinato livello di affidabilità, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informativi e di rete o accessibili attraverso di essi;

«**minaccia informatica**»: qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo su sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone, così come definita dall'articolo 2, punto 8), del regolamento (UE) 2019/881;

«**minaccia informatica significativa**»: una minaccia informatica che, in base alle sue caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informativi e di rete di un soggetto o sugli utenti dei servizi erogati da un soggetto causando perdite materiali o immateriali considerevoli;

DEFINIZIONI

«**incidente**»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi;

«**quasi-incidente**»: cd. *near-miss*, un evento che avrebbe potuto configurare un incidente senza che quest'ultimo si sia tuttavia verificato, ivi incluso il caso in cui l'incidente sia stato efficacemente evitato;

«**incidente di sicurezza informatica su vasta scala**»: un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri;

«**gestione degli incidenti**»: le azioni e le procedure volte a prevenire, rilevare, analizzare e contenere un incidente o a rispondervi e recuperare da esso;

GESTIONE DEL RISCHIO

ART. 23 ***(Organi di amministrazione e direttivi)***

1. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate da tali soggetti ai sensi dell'articolo 24;

b) sovrintendono all'implementazione degli obblighi di cui al presente capo e di cui all'articolo 7;

c) sono responsabili delle violazioni di cui al presente decreto.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

GESTIONE DEL RISCHIO

ART. 23 ***(Organi di amministrazione e direttivi)***

2. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti:

a) sono tenuti a seguire una formazione in materia di sicurezza informatica;

b) promuovono l'offerta periodica di una formazione coerente a quella di cui alla lettera a) ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti.

3. Gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche di cui agli articoli 25 e 26.

GESTIONE DEL RISCHIO

ART.24

I soggetti essenziali e i soggetti importanti adottano misure tecniche, operative e organizzative adeguate e proporzionate, secondo le modalità e i termini di cui agli articoli 30, 31 e 32, alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei loro servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi. Tali misure:

- *a)* assicurano un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia e, ove applicabile, delle pertinenti norme nazionali, europee e internazionali, nonché dei costi di attuazione;
- *b)* sono proporzionate al grado di esposizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

GESTIONE DEL RISCHIO

Le misure di gestione dei rischi dovrebbero **tenere conto del grado di dipendenza del soggetto essenziale o importante dai sistemi informatici e di rete e comprendere misure per individuare eventuali rischi di incidenti, per prevenire e rilevare incidenti, nonché per rispondervi, riprendersi da essi e attenuarne l'impatto**.

Nel valutare la proporzionalità di tali misure, si tiene debitamente conto:

- del grado di esposizione del soggetto a rischi,
- delle dimensioni del soggetto e
- della probabilità che si verifichino incidenti, nonché
- della loro gravità, compreso il loro impatto sociale ed economico.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

GESTIONE DEL RISCHIO

Le misure di gestione dei rischi di cibersicurezza dovrebbero essere basate su un «**approccio multirischio**» mirante **a proteggere i sistemi informatici e di rete e il loro ambiente fisico da eventi quali furti, incendi, inondazioni, problemi di telecomunicazione o interruzioni di corrente, o da qualsiasi accesso fisico non autorizzato** nonché **dai danni alle informazioni detenute dai soggetti essenziali o importanti e agli impianti di trattamento delle informazioni di questi ultimi**

GESTIONE DEL RISCHIO

Politiche di analisi dei rischi e di sicurezza dei sistemi informatici

Definire gli **obiettivi**

- Identificare le **aree di rischio** e identificare i **fornitori critici su quelle aree**
- Definire le **soglie di tolleranza**
  - Risk appetite (propensione al rischio)
  - Risk tolerance (devianza tollerabile rispetto alla propensione)
  - Risk capacity (massimo livello di rischio sopportabile)
- **Analizzare** il rischio (Probabilità e Impatti)
- **Valutare** il rischio rispetto alle soglie
- Identificare gli **indicatori di rischio** e i parametri di controllo (**KRI**)
- Identificare gli **indicatori di performance** e i parametri di controllo (**KPI**)
- Scegliere l'**azione di trattamento** dei rischi valutati
- **Monitoraggio** e **revisione** periodica

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

Quali sono i requisiti tecnici e metodologici delle misure per la gestione dei rischi in materia di cybersicurezza previsti dalla Direttiva NIS2?
Quando un incidente cyber deve essere considerato come 'significativo', ai sensi della Direttiva NIS2?

PRIMO REGOLAMENTO ATTUATIVO (Provvisorio. In attesa del parere del comitato composto dai rappresentanti degli Stati membri)

SOLO ai **fornitori di servizi DNS**, ai registri dei **nomi a dominio di primo livello**, ai fornitori di **servizi di cloud computing**, ai fornitori di **servizi di datacenter**, ai fornitori di **reti di distribuzione di contenuti**, ai fornitori di servizi gestiti (**managed service providers**), ai fornitori di servizi di sicurezza gestiti (**managed service security providers**), ai fornitori di **marketplace online**, di **motori di ricerca online** e di piattaforme di servizi di socialnetwork, così come ai prestatori di servizi fiduciari (**trust service providers**).

EUROPEAN
COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

tech metis

EVOLUMIA
The cyber security company

MÜSA
FORMAZIONE E LAVORO

Article 3 **Significant incidents**

(a) L'incidente ha causato o è in grado di causare perdite finanziarie dirette per l'entità pertinente che supera i 500 000 e euro o il 5 % del fatturato annuo totale dell'entità pertinente nell'esercizio precedente, a seconda di quale sia inferiore;

(b) L'incidente ha causato o è in grado di causare l'esfiltrazione di segreti commerciali come indicato nell'articolo 2 comma (1), della direttiva (UE) 2016/943 dell'entità pertinente;

(c) L'incidente ha causato o è in grado di causare la morte di una persona;

(d) L'incidente ha causato o è in grado di causare danni considerevoli alla salute di una persona;

(e) Si è verificato un accesso ai sistemi di informativi e di rete, che si sospetta essere dannoso e non autorizzato, che è in grado di causare una grave interruzione operativa;

EUROPEAN COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

ANNEX
3.5. Risposta agli incidenti

3.5.1. Le entità competenti devono rispondere agli incidenti in conformità con le procedure documentate e in modo tempestivo.

3.5.2. Le procedure di risposta agli incidenti devono includere le seguenti fasi:

a) contenimento dell'incidente, per impedire che le conseguenze dell'incidente si diffondano;
b) eradicazione, per impedire che l'incidente continui o si ripeta,
c) recupero dall'incidente, ove necessario.

EUROPEAN COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

ANNEX

3.5.3. Le entità pertinenti stabiliscono piani e procedure di comunicazione:

a) con i Computer Security Incident Response Team (CSIRT) o, ove applicabile, con le autorità competenti, in relazione alla notifica degli incidenti;
b) per la comunicazione tra i membri dello staff dell'entità pertinente e per la comunicazione con le parti interessate pertinenti esterne all'entità pertinente.

3.5.4. Le entità pertinenti registrano le attività di risposta agli incidenti in conformità alle procedure di cui al punto 3.2.1 e registrano le prove.

3.5.5. Le entità pertinenti testano a intervalli pianificati le proprie procedure di risposta agli incidenti.

EUROPEAN COMMISSION

Brussels, 17.10.2024
C(2024) 7151 final

COMMISSION IMPLEMENTING REGULATION (EU) …/...

of 17.10.2024

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

(Text with EEA relevance)

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

LE MISURE DI SICUREZZA

DELLA

NIS2

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

techmetis
EVOLUMIA The cyber security company
MÜSA FORMAZIONE E LAVORO

WEBINAR: NIS 2, Facciamo Chiarezza e Iniziamo ad Adeguarci

Cyber Security Framework

La function **RECOVER** è associata alla definizione e attuazione delle attività per la gestione dei piani e delle attività per il ripristino dei processi e dei servizi impattati da un incidente.
L'obiettivo è garantire la resilienza dei sistemi e delle infrastrutture e, in caso di incidente, supportare il recupero tempestivo delle business operations.
Le category all'interno di questa function sono:

Recovery Planning, Improvements, Communications.

La function **RESPOND** è associata alla definizione e attuazione delle opportune attività per intervenire quando un incidente di sicurezza informatica sia stato rilevato.
L'obiettivo è contenere l'impatto determinato da un potenziale incidente di sicurezza informatica.
Le category all'interno di questa function sono: Response Planning, Communications, Analysis, Mitigation, Improvements.

La function **IDENTIFY** è legata alla comprensione del contesto aziendale degli asset che supportano i processi critici di business e dei relativi rischi associati. Asset Management, Business Environment; Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management e Data Management

La function **PROTECT** è associata all'implementazione di quelle misure volte alla protezione dei processi di business e degli asset aziendali, indipendentemente dalla loro natura informatica. Le category all'interno di questa function sono: Identity Management, Authentication and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology.

La function **DETECT** è associata alla definizione e attuazione di attività appropriate per identificare tempestivamente incidenti di sicurezza informatica. Le category all'interno di questa function sono: Anomalies and Events, Security Continuous Monitoring, Detection Processes.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

tech metis
EVOLUMIA The cyber security company
MÜSA FORMAZIONE E LAVORO

MISURE DI SICUREZZA

politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete	politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica
gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche (artt. 25 e 26)	pratiche di igiene di base e di formazione in materia di sicurezza informatica
continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi	politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura
sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi	sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti
sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità	uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

sicurezza della catena di approvvigionamento

Considerando (85)

Affrontare i rischi derivanti dalla catena di approvvigionamento di un soggetto e dalla sua relazione con i fornitori, ad **esempio i fornitori di servizi di conservazione ed elaborazione dei dati o di servizi di sicurezza gestiti e gli editori di software,** è particolarmente importante data la prevalenza di incidenti in cui i soggetti sono stati vittime di attacchi informatici e in cui i responsabili di atti malevoli sono stati in grado di compromettere la sicurezza dei sistemi informatici e di rete di un soggetto sfruttando le vulnerabilità che interessano prodotti e servizi di terzi. I soggetti essenziali e importanti dovrebbero pertanto **valutare e tenere in considerazione la qualità e la resilienza complessive dei prodotti e dei servizi, delle misure di gestione dei rischi di cibersicurezza in essi integrate e delle pratiche di cibersicurezza dei loro fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro**.

In particolare, i soggetti essenziali e importanti dovrebbero essere incoraggiati a **integrare misure di gestione dei rischi di cibersicurezza negli accordi contrattuali con i loro fornitori e fornitori di servizi diretti. Tali soggetti potrebbero prendere in considerazione i rischi derivanti da altri livelli di fornitori e fornitori di servizi.**

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

sicurezza della catena di approvvigionamento

QUALI FORNITORI CONTROLLIAMO (Considerando 91)

Per individuare le catene di approvvigionamento che dovrebbero essere soggette a una valutazione coordinata dei rischi per la sicurezza, dovrebbero essere presi in considerazione i seguenti criteri:

- la misura in cui i soggetti essenziali e importanti ricorrono e si affidano a specifici servizi TIC, sistemi TIC o prodotti TIC critici;
- la pertinenza di specifici servizi TIC, sistemi TIC o prodotti TIC critici per lo svolgimento di funzioni critiche o sensibili, compreso il trattamento dei dati personali;
- la disponibilità di servizi TIC, sistemi TIC o prodotti TIC alternativi;
- la resilienza dell'intera catena di approvvigionamento di servizi TIC, sistemi TIC o prodotti TIC, durante tutto il loro ciclo di vita, contro eventi perturbatori e
- per i servizi TIC, sistemi TIC o prodotti TIC emergenti, la loro potenziale importanza futura per le attività dei soggetti. Inoltre, si dovrebbe porre un accento particolare sui servizi TIC, i sistemi TIC o i prodotti TIC che sono soggetti a requisiti specifici derivanti da paesi terzi.

sicurezza della catena di approvvigionamento

COSA CONTROLLIAMO

Art.24 comma 3

Nel valutare quali misure di cui al comma 2, lettera d), siano adeguate, i soggetti tengono conto delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro. Per la medesima finalità i soggetti tengono altresì conto dei risultati delle valutazioni coordinate dei rischi per la sicurezza delle catene di approvvigionamento critiche effettuate dal Gruppo di cooperazione NIS.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

sicurezza della catena di approvvigionamento

CHE MISURE DI TUTELA ADOTTIAMO

Valutazione ex ante del fornitore (verificare esistenza e adeguatezza politiche di sicurezza, valutare misure di sicurezza poste in essere, valutare la postura di sicurezza (CTI, Surface attack management), reputazione, qualità del prodotto/servizio, etc.)

Definire gli obblighi di sicurezza nei contratti, prevedendo ove possibile audit ed exit strategies in caso di non adempimento (Evitare lock-in tecnologico e assicurarsi possibilità di rescissione del contratto in caso il fornitore si rilevi inadeguato sotto il profilo della sicurezza)

Differenziare ove possibile il fornitore, utilizzando più fornitori per il prodotto servizio (non sempre è possibile) per limitare gli effetti di un problema di sicurezza legato dal fornitore

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

sicurezza della catena di approvvigionamento - RISORSE

NIST SP 800-161 Rev. 1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

https://csrc.nist.gov/pubs/sp/800/161/r1/final

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Gestione degli incidenti

ART. 25 *(Obblighi in materia di notifica di incidente)*

1. I soggetti essenziali e i soggetti importanti notificano, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che, ai sensi del comma 4, ha un impatto significativo sulla fornitura dei loro servizi, secondo le modalità e i termini di cui agli articoli 30, 31 e 32.

2. Le notifiche includono le informazioni che consentono al CSIRT Italia di determinare un eventuale impatto transfrontaliero dell'incidente.

……

4. Un incidente è considerato significativo se:

a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;

b) ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.

Notifica degli incidenti

ART. 25 *(Obblighi in materia di notifica di incidente)*

5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:

a) senza ingiustificato ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, una pre-notifica che, ove possibile, indichi se l'incidente significativo possa ritenersi il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;

b) senza ingiustificato ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, ove possibile, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione;

c) su richiesta del CSIRT Italia, una relazione intermedia sui pertinenti aggiornamenti della situazione;

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Notifica degli incidenti

ART. 25 *(Obblighi in materia di notifica di incidente)*

5. Ai fini della notifica di cui al comma 1, i soggetti interessati trasmettono al CSIRT Italia:

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

- 1) una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
- 2) il tipo di minaccia o la causa originale (*root cause*) che ha probabilmente innescato l'incidente;
- 3) le misure di attenuazione adottate e in corso;
- 4) ove noto, l'impatto transfrontaliero dell'incidente;

e) in caso di incidente in corso al momento della trasmissione della relazione finale di cui alla lettera d), una relazione mensile sui progressi e una relazione finale entro un mese dalla conclusione della gestione dell'incidente.

RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Notifica degli incidenti

ART. 25 *(Obblighi in materia di notifica di incidente)*

6. In deroga a quanto previsto dal comma 5, lettera b), un prestatore di servizi fiduciari, in relazione a incidenti significativi che abbiano un impatto sulla fornitura dei suoi servizi fiduciari, provvede alla notifica di cui alla medesima lettera, senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo. (anziché 72 ore, ndr)

7. Fermo restando quanto previsto dall'articolo 15, comma 4*, senza ingiustificato ritardo e ove possibile entro 24 ore dal ricevimento della pre-notifica di cui al comma 5, lettera a), il CSIRT Italia fornisce una risposta al soggetto notificante, comprensiva di un riscontro iniziale sull'incidente significativo e, su richiesta del soggetto, orientamenti o consulenza sull'attuazione di possibili misure tecniche di mitigazione. Su richiesta del soggetto notificante, il CSIRT Italia fornisce ulteriore supporto tecnico.

* Il CSIRT Italia applica un approccio basato sul rischio per stabilire l'ordine di priorità nello svolgimento dei suoi compiti

Notifica degli incidenti

Art.25

9. Sentito il CSIRT Italia, se ritenuto opportuno e qualora possibile, i soggetti essenziali e i soggetti importanti comunicano, senza ingiustificato ritardo, ai destinatari dei loro servizi gli incidenti significativi che possono ripercuotersi negativamente sulla fornitura di tali servizi.

10. I soggetti essenziali e i soggetti importanti, se ritenuto opportuno e qualora possibile, sentito il CSIRT Italia, comunicano senza ingiustificato ritardo, ai destinatari dei loro servizi che sono potenzialmente interessati da una minaccia informatica significativa, misure o azioni correttive o di mitigazione che tali destinatari possono adottare in risposta a tale minaccia. Inoltre, sentito il CSIRT Italia, se ritenuto opportuno, i soggetti essenziali e i soggetti importanti comunicano ai medesimi destinatari anche la natura di tale minaccia informatica significativa.

Notifica degli incidenti

ART. 26 ***(Notifica volontaria di informazioni pertinenti)***

1. In aggiunta all'obbligo di notifica di incidente di cui all'articolo 25, possono essere trasmesse, su base volontaria, notifiche al CSIRT Italia da parte dei:

a) **soggetti essenziali e soggetti importanti**, per quanto riguarda gli
- incidenti diversi da quelli di cui all'articolo 25, comma 1,
- le minacce informatiche e
- i quasi-incidenti;

b) **soggetti diversi** da quelli di cui alla lettera a), **indipendentemente dal fatto che ricadano o meno nell'ambito di applicazione del presente decreto**, per quanto riguarda gli incidenti che hanno un impatto significativo sulla fornitura dei loro servizi, le minacce informatiche e i quasi-incidenti.

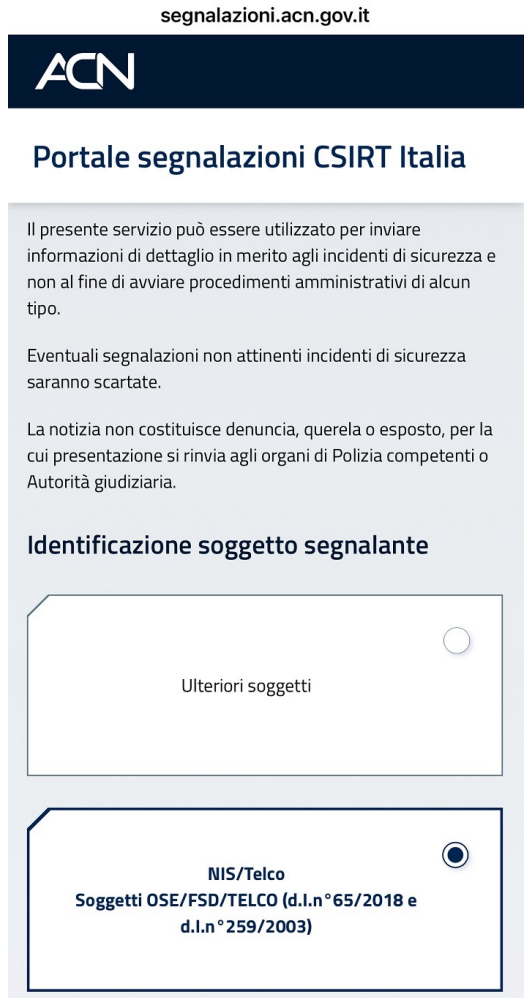
RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

Notifica degli incidenti

Link per la segnalazione degli incidenti

https://www.csirt.gov.it/segnalazione

https://www.acn.gov.it/portale/documents/d/guest/acn_guida_notifica_incidenti_clear-pdf



RELATORE: Lino Fornaro - Senior Security Manager
l.fornaro@evolumia.it

tech metis
EVOLUMIA The cyber security company
MÜSA FORMAZIONE E LAVORO

Grazie

Lino Fornaro
Security Manager
EVOLUMIA SRL

l.fornaro@evolumia.it – 393 3364920