MINISTERO DELLO SVILUPPO ECONOMICO

DECRETO 12 dicembre 2018

Misure di sicurezza ed integrita' delle reti di comunicazione elettronica e notifica degli incidenti significativi. (19A00317)

(GU n.17 del 21-1-2019)

IL MINISTRO
DELLO SVILUPPO ECONOMICO

Visto il decreto legislativo 1° agosto 2003, n. 259, recante il Codice delle comunicazioni elettroniche, modificato dal decreto legislativo 28 maggio 2012, n. 70 in attuazione delle direttive 2009/140/CE in materia di reti e servizi di comunicazione elettronica e 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata;

Visti in particolare, gli articoli 16-bis e 16-ter del predetto decreto legislativo n. 259 del 2003 e successive modificazioni;

Vista la legge 3 agosto 2007, n. 124, recante il sistema di informazione per la sicurezza della Repubblica e la nuova disciplina del segreto;

Vista la direttiva adottata con decreto del Presidente del Consiglio dei ministri del 17 febbraio 2017, recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali, pubblicato nella Gazzetta Ufficiale n. 87 del 13 aprile 2017;

Visto il decreto legislativo 18 maggio 2018, n. 65, che ha recepito la direttiva (UE) 2016/1148 in materia di sicurezza delle reti e dei sistemi informativi, ed in particolare l'art. 8 e l'art. 12, comma 6 relativi rispettivamente al CSIRT Italiano e all'organo istituito presso il Dipartimento informazioni per la sicurezza incaricato, ai sensi delle direttive del Presidente del Consiglio dei ministri adottate sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), delle attivita' di prevenzione e preparazione ad eventuali situazioni di crisi e di attivazione delle procedure di allertamento;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante il «Codice in materia di protezione dei dati personali»;

Visto il decreto del Ministro delle comunicazioni di concerto con il Ministro dell'economia e delle finanze del 15 febbraio 2006, pubblicato nella Gazzetta Ufficiale del 7 aprile 2006, n. 82, e relativo ai compensi dovuti per prestazioni conto terzi eseguite dal Ministero delle comunicazioni, ai sensi dell'art. 6 del decreto legislativo 30 dicembre 2003, n. 366;

Visto il decreto della Presidenza del Consiglio dei ministri 5 dicembre 2015, n. 158, recante il Regolamento di organizzazione del Ministero dello sviluppo economico, ed in particolare l'art. 14 che affida all'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione l'individuazione delle misure tecnico-organizzative di sicurezza ed integrita' delle reti, la verifica del rispetto delle stesse e la notifica degli incidenti di sicurezza significativi agli organi europei competenti, ai sensi degli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, in accordo con i soggetti istituzionali competenti e, in particolare, con l'Agenzia per l'Italia Digitale;

Vista la legge 31 luglio 1997, n. 249, recante «Istituzione dell'Autorita' per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo» e, in particolare,

l'art. 1;

Tenuto conto delle indicazioni contenute nei documenti elaborati dall'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) con il contributo degli Stati membri dell'Unione europea: «Technical guidance on the security measures in Article 13a» -Versione 2.0, Ottobre 2014 e «Technical guidance on the incident reporting in Article 13» Versione 2.1, Ottobre 2014;

Considerata la necessita' di attuare le disposizioni dei suddetti articoli 16-bis e 16-ter, al fine di incrementare i livelli di sicurezza delle reti e la disponibilita' dei servizi su tali reti;

Considerati i dati pubblicati nell'Osservatorio trimestrale delle comunicazioni a cura dell'Autorita' per le garanzie nelle comunicazioni relativamente alla base di utenti nazionali per i servizi voce e dati su rete fissa e rete mobile;

Sentiti i fornitori di reti e servizi di comunicazione elettronica e le relative Associazioni;

Sentite l'Autorita' per le garanzie nelle comunicazioni e l'Agenzia per l'Italia Digitale;

Decreta:

Art. 1

Definizioni

1. Ai fini del presente decreto si intende per:

a) «incidente di sicurezza»: una violazione della sicurezza o perdita dell'integrita' che determina un malfunzionamento delle reti e dei servizi di comunicazione elettronica;

b) «asset critico»: un'infrastruttura in grado di fornire servizi di comunicazione elettronica a un significativo numero di utenti, espresso in termini percentuali rispetto alla base di utenti nazionale dei medesimi servizi;

c) «sicurezza e integrita' della rete»: condizioni che assicurano la disponibilita' e continuita' dei servizi di comunicazioni elettroniche forniti;

d) «base di utenti nazionale»: il numero totale di utenti finali a livello nazionale per singolo servizio di comunicazioni elettroniche, da intendersi come:

numero di accessi complessivi da rete fissa (sia voce che dati);

numero complessivo delle SIM attive Human (per traffico voce e dati).

2. Per quanto non espressamente previsto dal comma 1, si applicano le definizioni del decreto legislativo 1° agosto 2003, n. 259, recante il «Codice delle comunicazioni elettroniche».

Art. 2

Scopo del decreto

1. Il presente decreto attua le disposizioni degli articoli 16-bis e 16-ter del decreto legislativo 1° agosto 2003, n. 259, e, in particolare, persegue i seguenti obiettivi:

a) individuare adeguate misure di natura tecnico - organizzativa per la sicurezza e l'integrita' delle reti e dei servizi di comunicazione elettronica, al fine di conseguire un livello di sicurezza delle reti adeguato al rischio esistente e di garantire la disponibilita' e continuita' dei servizi su tali reti, prevenendo e limitando gli impatti di incidenti che possono pregiudicare la sicurezza per gli utenti e per le reti interconnesse;

b) definire i casi in cui le violazioni della rete o la perdita dell'integrita' sono da considerarsi significative, ai fini della notifica da parte dei fornitori di reti e servizi di comunicazione alle competenti Autorita', nonche' le relative modalita' di tale

notifica.

Art. 3

Campo di applicazione

1. Il presente decreto si applica ai servizi di comunicazione elettronica di seguito riportati:

a) accesso alla rete fissa o mobile da postazione fissa;

b) accesso alla rete fissa o mobile da terminale mobile.

2. Il presente decreto si applica ai fornitori di reti e servizi di comunicazione elettronica che servono un numero di utenti effettivo pari o superiore all'1% della base di utenti nazionale per ciascun servizio di cui al comma 1, calcolato sulla base dei dati pubblicati dall'Osservatorio trimestrale delle comunicazioni a cura dell'Autorita' per le garanzie nelle comunicazioni. Il presente decreto si applica altresi' ai fornitori di reti e servizi di comunicazione elettronica che servono un numero di utenti effettivo pari o superiore ad un milione.

Art. 4

Misure di sicurezza e integrita' delle reti

1. I fornitori di reti e servizi di comunicazione elettronica sono tenuti ad adottare le seguenti misure di sicurezza e integrita' delle reti e dei servizi:

a) politica di sicurezza approvata dalla Direzione aziendale:

1) predisporre una documentata politica relativamente alla sicurezza e alla integrita' delle reti di comunicazione e dei servizi forniti;

2) definire una dettagliata politica di sicurezza per gli asset critici e i processi aziendali;

3) definire e mantenere aggiornata una politica di sicurezza per tutti gli aspetti elencati nelle successive lettere;

b) gestione del rischio:

1) individuare i principali rischi per la sicurezza e l'integrita' delle reti e dei servizi di comunicazione elettronica forniti, tenendo conto delle minacce che insistono sugli asset critici;

2) definire una metodologia di gestione dei rischi e utilizzare strumenti basati sugli standard di settore;

3) verificare l'effettivo utilizzo di tali metodologie e strumenti di gestione del rischio da parte del personale;

4) assicurarsi che i rischi residui, anche derivanti da vincoli realizzativi, siano minimizzati rispetto alla probabilita' del verificarsi di incidenti significativi e che siano accettati dalla Direzione;

c) struttura organizzativa:

1) identificare ruoli per il personale e le relative responsabilita' in autonomia di esercizio;

2) conferire, con formale nomina, ruoli e responsabilita' al personale;

3) assicurare la reperibilita', in caso di incidenti di sicurezza, del personale responsabile;

d) servizi e prodotti forniti da terze parti:

1) definire i requisiti di sicurezza nei contratti con terze parti;

2) verificare il rispetto dei requisiti fissati nei contratti;

3) assicurare che i rischi residui che non sono gestiti dalla terza parte siano minimizzati rispetto alla probabilita' del verificarsi di incidenti e che siano accettati dalla Direzione;

4) tenere traccia ed eventualmente gestire gli incidenti di sicurezza relativi a terze parti o da esse causati che si ripercuotono sulla rete o sul servizio erogato;

e) formazione e gestione del personale:

1) definire un piano di formazione del personale;

2) prevedere un'adeguata ed aggiornata formazione del personale con ruoli di responsabilita';
3) organizzare corsi di formazione e sessioni di sensibilizzazione per tutto il personale;
4) verificare le conoscenze acquisite dal personale;
5) definire appropriate procedure per gestire le nuove assunzioni e la rotazione del personale che ricopre ruoli di responsabilita';
6) revocare diritti di accesso, se non piu' giustificati;
7) definire procedure di intervento per violazioni delle politiche di sicurezza di cui alla lettera a), che mettano a rischio la sicurezza e l'integrita' delle reti e dei servizi di comunicazione elettronica;

f) sicurezza fisica e logica:

1) definire condizioni, responsabilita' e procedure per l'assegnazione, la revoca dei diritti di accesso, e per l'approvazione delle eventuali eccezioni;
2) definire meccanismi di autenticazione appropriati, a seconda del tipo di accesso;
3) adottare meccanismi di protezione da accessi fisici non autorizzati o da eventi imprevisti quali, a titolo esemplificativo ma non esaustivo, furti con scasso, incendi, inondazioni;
4) adottare meccanismi di controllo di accesso logico appropriati per l'accesso alla rete e ai sistemi di informazione per consentirne solo l'uso autorizzato;
5) verificare che utenti e sistemi abbiano ID univoci e possano accedere ad altri servizi e sistemi previa autenticazione;
6) monitorare e registrare gli accessi;
7) prevedere meccanismi di protezione degli impianti funzionali all'erogazione del servizio, quali, a titolo esemplificativo ma non esaustivo, elettricita' e gas;

g) integrita' della rete e dei sistemi informativi:

1) implementare sistemi di protezione e di rilevamento di codice malevolo che possa alterare la funzionalita' dei sistemi;
2) assicurarsi che il software impiegato nella rete e nei sistemi informativi non venga manomesso o alterato;
3) assicurarsi che i dati critici sulla sicurezza, quali, a titolo esemplificativo ma non esaustivo, password e chiavi private, non siano divulgati o manomessi;

h) gestione operativa:

1) predisporre le procedure operative e individuare i responsabili per il funzionamento dei sistemi critici;
2) predisporre procedure per la gestione di eventuali cambiamenti;
3) attenersi alle procedure predefinite quando si effettuano attivita' sui sistemi critici;
4) registrare e documentare ogni modifica o attivita' effettuata sui sistemi critici;
5) predisporre e aggiornare un database delle configurazioni dei sistemi critici per eventuali ripristini delle stesse;
6) predisporre e aggiornare un inventario degli asset critici;

i) gestione degli incidenti di sicurezza:

1) prevedere una struttura tecnica con adeguata competenza e disponibilita' incaricata della gestione degli incidenti;
2) predisporre e aggiornare un database degli incidenti;
3) esaminare i principali incidenti e redigere relazioni sugli stessi, che contengano informazioni sulle azioni intraprese e sulle raccomandazioni per ridurre il rischio del ripetersi di incidenti analoghi;
4) definire e implementare processi e sistemi per il rilevamento degli incidenti;
5) definire procedure per informare gli utenti su incidenti in corso o risolti, oltreche' il CSIRT italiano e l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione del

Ministero dello sviluppo economico (di seguito anche ISCTI) secondo quanto previsto dal presente decreto, notiziando comunque preventivamente il CSIRT e l'ISCTI;

6) definire procedure per la segnalazione degli incidenti significativi ai sensi del successivo art. 5.

j) continuita' operativa:

1) predisporre e implementare piani di emergenza per gli asset critici;

2) monitorare l'attivazione e l'esecuzione di piani di emergenza, registrando i tempi di ripristino dell'operativita' e del servizio;

3) predisporre e mantenere una appropriata capacita' di disaster recovery;

4) implementare procedure per le attivita' di ripristino dell'operativita' e dei servizi;

k) monitoraggio, test e controllo:

1) sottoporre a test reti, sistemi informativi e nuove versioni del software prima di utilizzarli o collegarli a sistemi esistenti;

2) implementare il monitoraggio e la registrazione dello stato e degli eventi dei sistemi critici;

3) impostare gli strumenti per raccogliere e archiviare i registri dei sistemi critici;

4) configurare strumenti per la raccolta e l'analisi automatizzata di dati e registri di monitoraggio;

5) predisporre un programma per la realizzazione di esercitazioni periodiche per testare piani di disaster recovery e di ripristino dei backup;

6) implementare strumenti per test automatizzati;

7) assicurarsi che i sistemi critici siano sottoposti a scansioni e test di sicurezza regolarmente, in particolare quando vengono introdotti nuovi sistemi e in seguito a modifiche;

8) monitorare la conformita' agli standard e alle disposizioni normative.

2. Le misure di cui al comma 1 si riferiscono agli asset critici, individuati secondo le modalita' di cui all'Allegato 1 al presente decreto, in cui il valore della percentuale dell'utenza, che l'asset e' potenzialmente in grado di servire per ciascun servizio di cui al comma 1, e' pari o superiore all'1% della base di utenti nazionale per quel servizio, sulla base dei dati pubblicati dall'Osservatorio trimestrale delle comunicazioni a cura dell'Autorita' per le garanzie nelle comunicazioni. Le misure di cui al comma 1 si riferiscono altresi' agli asset critici individuati secondo i criteri di cui all'Allegato 1 al presente decreto in cui il numero della potenziale utenza servita e' pari o superiore ad un milione.

Art. 5

Incidenti significativi

1. I parametri che definiscono la significativita' di un incidente di sicurezza sono la durata del disservizio e la percentuale degli utenti colpiti rispetto al totale degli utenti nazionali del servizio interessato.

2. In attuazione dei parametri di cui all'art. 3, comma 2, gli incidenti sono da considerarsi significativi, nei seguenti casi:

a) durata superiore ad un'ora e percentuale degli utenti colpiti superiore al quindici per cento del totale degli utenti nazionali del servizio interessato;

b) durata superiore a due ore e percentuale degli utenti colpiti superiore al dieci per cento del totale degli utenti nazionali del servizio interessato;

c) durata superiore a quattro ore e percentuale degli utenti colpiti superiore al cinque per cento del totale degli utenti nazionali del servizio interessato;

d) durata superiore a sei ore e percentuale degli utenti colpiti superiore al due per cento del totale degli utenti nazionali del servizio interessato;

e) durata superiore ad otto ore e percentuale degli utenti colpiti superiore all'uno per cento del totale degli utenti nazionali del servizio interessato.

3. Nei casi di cui al comma 2, i fornitori di servizi di comunicazione elettronica segnalano tempestivamente l'incidente al CSIRT di cui all'art. 8 del decreto legislativo 18 maggio 2018, n. 65 e all'ISCTI. La comunicazione e' effettuata entro ventiquattro ore dall'avvenuta rilevazione dell'incidente, con l'indicazione almeno delle seguenti informazioni, qualora disponibili:

a) servizio interessato;

b) durata dell'incidente qualora concluso, ovvero la stima della conclusione se ancora in corso;

c) impatto stimato sull'utenza del servizio interessato in termini percentuali rispetto alla base di utenti nazionale per il medesimo servizio.

4. Entro cinque giorni dalla segnalazione di cui al comma 3, i fornitori di servizi di comunicazione elettronica trasmettono al CSIRT e all'ISCTI un rapporto in cui sono riportati:

a) descrizione dell'incidente;

b) causa dell'incidente quale, a titolo meramente esemplificativo ma non esaustivo, errore umano, guasto, fenomeno naturale, azioni malevoli, guasti causati da terze parti;

c) conseguenze sul servizio fornito;

d) infrastrutture e sistemi colpiti;

e) impatto sulle interconnessioni a livello nazionale;

f) azioni di risposta per mitigare l'impatto dell'incidente;

g) azioni per ridurre la probabilita' del ripetersi dell'incidente o di incidenti simili.

Eventuali informazioni rilevanti emerse successivamente all'invio del suddetto rapporto saranno oggetto di un rapporto integrativo trasmesso con la massima sollecitudine al CSIRT e all'ISCTI.

5. L'ISCTI inoltra tempestivamente le comunicazioni di cui ai commi 3 e 4 all'organo di cui all'art. 12, comma 6, del decreto legislativo 18 maggio 2018, n. 65.

6. L'ISCTI invia all'Agenzia ENISA e alla Commissione europea con periodicita' annuale un report sugli incidenti segnalati, contenente le informazioni di cui ai commi 3 e 4, senza l'indicazione dei fornitori di reti e servizi di comunicazione elettronica interessati.

7. Nei casi in cui gli incidenti di cui al comma 3 possono avere un impatto su reti e servizi di un altro Stato membro, i fornitori di reti e servizi di comunicazione elettronica informano tempestivamente il CSIRT e l'ISCTI per la successiva notifica all'Agenzia ENISA e all'Autorita' dello Stato membro interessato.

Art. 6

Rispetto degli obblighi

1. Entro novanta giorni dall'entrata in vigore del presente decreto, i fornitori di reti e servizi di comunicazione elettronica trasmettono all'ISCTI l'elenco degli asset critici oggetto delle misure di cui all'art. 4, individuati secondo i criteri stabiliti nell'Allegato 1, e implementano tali misure nei successivi centoventi giorni.

2. Ai fini della valutazione del soddisfacimento delle misure definite nell'art. 4, comma 1 del presente decreto, l'ISCTI tiene conto anche dell'eventuale possesso di certificazioni di conformita' a standard riconosciuti a livello internazionale che attestano l'applicazione di tali misure.

3. Al fine di verificare la corretta applicazione delle disposizioni contenute nel presente decreto, l'ISCTI puo',

autonomamente o su impulso dell'Autorita' per le garanzie nelle comunicazioni, effettuare verifiche e controlli presso le sedi dei fornitori di reti e servizi di comunicazione elettronica, anche avvalendosi degli Ispettorati territoriali o di un organismo qualificato indipendente.

Ai sensi dell'art. 16-ter, comma 2, lettera b), del decreto legislativo 1° agosto 2003, n. 259, i relativi oneri finanziari sono sostenuti dai fornitori di reti e servizi di comunicazione elettronica.

Qualora dette attivita' ispettive siano eseguite da personale del Ministero dello sviluppo economico si applica un rimborso delle spese sostenute calcolato sulla base delle disposizioni contenute nel decreto 15 febbraio 2006 del Ministro delle comunicazioni di concerto con il Ministro dell'economia e delle finanze.

4. Qualora a seguito delle verifiche e dei controlli di cui al comma 3 venga riscontrata la mancata applicazione delle disposizioni del presente decreto, l'ISCTI diffida i fornitori di reti e servizi di comunicazione elettronica a regolarizzare la propria posizione entro un termine congruo decorso il quale, in caso di inottemperanza, trovano applicazione le sanzioni di cui all'art. 98, commi da 4 a 12, del decreto legislativo 1° agosto 2003, n. 259.

Art. 7

Disposizioni finali

1. Dall'attuazione del presente decreto non devono derivare nuovi o maggiori oneri per la finanza pubblica.

2. Il presente decreto e' modificato almeno ogni due anni.

3. Il presente decreto entra in vigore il giorno successivo alla sua pubblicazione nella Gazzetta Ufficiale della Repubblica italiana.

Roma, 12 dicembre 2018

Il Ministro: Di Maio

Allegato 1

Modalita' per l'individuazione degli asset critici di cui all'art. 4, comma 2

Il presente allegato si applica a ciascun servizio di cui all'art. 3, comma 1.

1. Identificazione degli asset.

Valutazione degli asset utilizzati per erogare i servizi di cui all'art. 3, comma 1, identificando per ciascuno di tali servizi tutti gli asset, propri o di terzi, che contribuiscono anche parzialmente alla fornitura dei servizi alla propria base di utenti.

2. Descrizione degli asset.

Individuazione degli asset identificati in termini funzionali e architetturali per ciascun servizio di cui all'art. 3, comma 1, sulla base della seguente ripartizione di elementi funzionali:

a) accesso (concentratori di rete fissa e apparati della rete radio di accesso);

b) commutazione (autocommutatori, router);

c) trasporto (apparati e cavi della rete ottica);

d) controllo e gestione (sistemi di segnalazione, sistemi di autenticazione, Domain Name System - DNS, Home Location Register - HLR, sistemi di gestione di rete).

3. Topologia, caratteristiche e distribuzione degli asset nella rete.

a) Identificazione degli asset in termini topologici e dimensionali nella rete relativamente alle tipologie di elementi funzionali definite al punto precedente;

b) distribuzione geografica e caratteristiche di ridondanza degli asset che compongono le tipologie degli elementi;

c) numerosita' dei suddetti asset;

d) interconnessioni tra i suddetti asset.

4. Esclusione degli asset.

Individuazione degli asset dei quali, sulla base di opportune motivazioni, si prevede l'esclusione dall'insieme di quelli oggetto della valutazione.