Direttiva UE

SICUREZZA DELLA RETE E DELLE INFORMAZIONI

cepAnalisi Nr. 13/2021

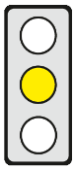
Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

PUNTI CHIAVE

Contesto: La Commissione ha identificato diverse debolezze nell'attuale Direttiva NIS (Network and Information Security). Intende porvi rimedio con nuovi standard di cibersicurezza.

Scopo della Direttiva: La Commissione UE vuole migliorare il livello di sicurezza informatica nell'UE.

Parti interessate: Grandi e importanti istituzioni private e pubbliche, agenzie e organismi di cibersicurezza europei e nazionali.



Pro: (1) Perseguire elevati livelli di sicurezza informatica per le imprese che sono cruciali per il funzionamento di una società appare un'iniziativa appropriata perché gli stimoli economici per investire nella sicurezza informatica risultano insufficienti e i costi per la società derivati da incidenti informatici che colpiscono imprese essenziali o importanti sono particolarmente elevati.

(2) Le nuove «procedure di segnalazione» aumentano la certezza giuridica e le strutture centrali di informazione riducono l'onere amministrativo per le entità tenute alla segnalazione.

Contro: (1) I nuovi obblighi per le aziende essenziali e importanti, di prendere in considerazione i rischi della catena di approvvigionamento dovrebbero essere limitati ai rischi che riguardano i fornitori di prodotti e servizi ICT considerati rilevanti per la sicurezza dell'attività delle aziende.

(2) L'obbligo di segnalare gli incidenti entro 24 ore potrebbe rivelarsi troppo oneroso.

I passaggi più importanti del testo sono evidenziati da una riga verticale a margine.

CONTENUTO

Titolo

Proposta COM(2020) 823 del 16 dicembre 2020 per una **Direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la Direttiva (UE) 2016/1148**

Breve riepilogo

- **Contesto e obiettivi**
  - La Direttiva sulla Sicurezza delle Reti e delle Informazioni ["NIS 1.0", (UE) 2016/1148, s.cep**Analisi**] prevede che:
    - gli Stati membri debbano instaurare strategie nazionali di cibersicurezza e designare autorità di cibersicurezza ;
    - vadano creati vari forum per migliorare la cooperazione in materia di sicurezza informatica tra gli Stati membri ;
    - gli Stati membri debbano stabilire regole vincolanti per la gestione del rischio di sicurezza informatica; e
    - gli Stati membri debbano fissare obblighi di segnalazione per gli incidenti relativi alla cibersicurezza.
  - Secondo la Commissione, la resilienza informatica dell'UE è migliorata notevolmente dall'entrata in vigore della Direttiva. Tuttavia, questa ha anche identificato alcune debolezze: [Considerando 2, pp. 5 e 6]
    - La portata della Direttiva è "troppo limitata" e "non fornisce sufficiente chiarezza";
    - Gli Stati membri hanno troppa discrezione nell'attuazione dei requisiti di gestione del rischio di sicurezza informatica e degli obblighi di segnalazione degli incidenti;
    - Le disposizioni di supervisione e di applicazione non sono "efficaci".
  - La proposta di Direttiva " NIS 2.0" affronta queste debolezze e abroga l'attuale Direttiva NIS.
- **Ambito di applicazione**
  - La Direttiva si applica a tutti gli enti pubblici e privati con più di 50 dipendenti o un fatturato annuo o un bilancio annuale di almeno €10 milioni, purché siano classificati come (vedi tabella CEP allegata per la lista completa in inglese) [Art. 2(1)] :
    - soggetti "essenziali", per esempio, servizi di elettricità e acqua, produttori di petrolio, banche; o
    - soggetti "importanti", ad esempio, produttori di dispositivi medici, produttori di alimenti o operatori di mercati online.
  - Indipendentemente dalle dimensioni, la Direttiva si applica agli enti pubblici e privati "essenziali" o "importanti" che [Art. 2 comma] :
    - sono fornitori di reti e servizi pubblici di comunicazione elettronica, servizi fiduciari o registri e sistemi di nomi di dominio di primo livello (TLD),

Autori: Philipp Eckhardt e Dr. Martina Anzini | eckhardt@cep.eu
Traduzione in italiano: Prof. Andrea De Petris
cep | Kaiser-Joseph-Straße 266 | 79098 Freiburg | Deutschland | Telefon + 49 761 38693-107 | www.cep.eu

- Le amministrazioni pubbliche dei governi centrali, delle grandi regioni socioeconomiche e delle entità amministrative che, tra l'altro, hanno personalità giuridica, sono stabilite per soddisfare scopi di interesse generale e possono prendere decisioni amministrative o regolamentari che influiscono sulla libera circolazione delle persone, delle merci, dei servizi e dei capitali,
- sono l'unico fornitore di un servizio in uno Stato membro,
- sono fornitori di servizi:
  - il cui turbamento potrebbe mettere in pericolo la sicurezza pubblica, l'ordine o la salute, o la stabilità del sistema transfrontaliero, o
  - che sono particolarmente critici a livello regionale o nazionale, o
  - identificati dagli Stati membri come "critici", cioè essenziali per il mantenimento di attività sociali o economiche essenziali, conformemente alla Proposta di Direttiva sulla resilienza dei soggetti critici [COM(2020) 829].

– I requisiti di gestione del rischio e di segnalazione della Direttiva non si applicano quando altre legislazioni dell'UE prevedono requisiti più stringenti [Art. 2(6)]. Questo vale, per esempio, per le entità del settore finanziario soggette alla Proposta di Regolamento relativo alla resilienza operativa digitale [COM(2020) 595, v. cep**Analisi**] [Considerando 13].

► **Gestione del rischio di cibersicurezza da parte di aziende essenziali e importanti**

– Le imprese di primaria importanza e significative devono adottare "misure tecniche e organizzative appropriate e proporzionate" per gestire i rischi alla sicurezza della Rete e dei sistemi informativi (NIS) che usano per fornire i loro servizi. Questo deve includere, come minimo, l'analisi dei rischi, le politiche di sicurezza dei sistemi informativi, la gestione degli incidenti, la continuità aziendale, la sicurezza della catena di approvvigionamento e l'uso della crittografia [Art. 18(1) e (2)].
– Per quanto riguarda la sicurezza delle loro catene di approvvigionamento, le imprese essenziali e importanti devono prendere in considerazione le vulnerabilità specifiche di ogni fornitore, così come la qualità dei prodotti dei fornitori e le pratiche di sicurezza informatica [Art. 18 comma 3].
– Gli organi direttivi delle aziende essenziali e importanti devono approvare le misure di gestione del rischio e monitorare la loro attuazione. Sono responsabili di qualsiasi inosservanza e devono fornire una formazione regolare sui rischi di cybersecurity e il loro impatto sul business [Art. 17].
– La Commissione può adottare atti attuativi per definire le "specifiche tecniche e metodologiche" delle misure di gestione del rischio, nonché atti delegati per estendere l'elenco delle misure [articolo 18, paragrafi 5 e 6].
– La Commissione può decidere - tramite atti delegati - che certe categorie di entità essenziali devono ottenere un certificato di sicurezza informatica per prodotti, servizi o processi ICT sotto specifici schemi europei di certificazione della sicurezza informatica (vedi anche cep**Analisi**). Gli Stati membri possono inoltre richiedere a singole entità essenziali e importanti di farlo [Art. 21].

► **Segnalazione di incidenti e minacce informatiche alle autorità e agli utenti dei servizi**

– Le strutture essenziali e importanti devono riferire prontamente alle autorità nazionali competenti o ai team nazionali di intervento per la sicurezza informatica (CSIRT - Computer Security Incident Response Team) qualsiasi incidente significativo [Art. 20] su:
  - incidenti informatici, ovvero quegli incidenti che potrebbero provocare una significativa interruzione dell'attività o una perdita finanziaria per l'azienda o una significativa perdita tangibile o intangibile per altri individui o entità;
  - minacce informatiche che avrebbero potuto potenzialmente provocare un incidente informatico significativo.
– Gli incidenti informatici significativi devono essere generalmente segnalati entro 24 ore, indicando se un incidente è "ritenuto il risultato di atti illeciti o dolosi" [Art. 20(4)].
– Su richiesta di un'autorità competente o del CSIRT, deve essere fornito un rapporto intermedio con aggiornamenti sullo stato di avanzamento [Art. 20(4)].
– Entro un mese da un incidente, deve essere presentato un rapporto finale che descriva la gravità e l'impatto dell'incidente, la natura della minaccia, la causa e le azioni correttive adottate [Art. 20 comma 4].
– Le strutture essenziali e importanti devono informare senza indugio i loro utenti del servizio [Art.20 comma1 e 2]
  - incidenti informatici che potrebbero influenzare la fornitura dei loro servizi, e
  - minacce informatiche significative e azioni che potrebbero intraprendere in risposta ad esse.
– Le autorità competenti o il CSIRT devono fornire un primo feedback entro 24 ore e, su richiesta dell'entità, fornire assistenza per intraprendere azioni correttive [Art. 20(5)].
– Le autorità competenti o il CSIRT possono informare il pubblico sull'incidente o chiedere alla struttura interessata di farlo, a condizione che la sensibilizzazione del pubblico possa prevenire l'incidente, contribuire alla sua gestione o essere nell'interesse pubblico [Art. 20(7)].
– Gli Stati membri dovrebbero istituire uno sportello unico nazionale per tutte le notifiche, che dovrebbe anche coprire, ad esempio, le notifiche di violazioni del regolamento generale sulla protezione dei dati [GDPR, (UE) 2016/679] e la Direttiva sulla ePrivacy [2002/58/CE] [considerando 56].

Autori: Philipp Eckhardt e Dr. Martina Anzini | Telefon + 49 761 38693-107| eckhardt@cep.eu
Traduzione in italiano: Prof. Andrea De Petris

- **Supervisione, applicazione e sanzioni**
  - Alle autorità nazionali competenti deve essere concesso un insieme minimo di poteri di supervisione, tra cui ispezioni in loco ed audit di sicurezza. Le strutture essenziali sono soggette alla supervisione ex-ante ed ex-post, quelle importanti solo alla supervisione ex-post. [Art. 29(2)e 30(2)]
  - Le autorità devono anche essere dotate di una serie minima di poteri di applicazione, anche per emettere avvertimenti e istruzioni. Queste possono essere dirette sia alle strutture essenziali che a quelle importanti. [art. 29(4) e art. 30(4)].
  - Se le aziende non rispettano le misure di applicazione, le autorità possono imporre sanzioni, che possono essere imposte alle entità e alle persone responsabili della loro gestione. [Art. 29(5)].

Cambiamenti significativi dello status quo

- Il NIS 2.0 copre una serie di entità e settori che non erano coperti dal NIS 1.0, ad esempio gli operatori di produzione di idrogeno, le società di acque reflue e i produttori di automobili (vedi tabella CEP allegata in inglese).
- La NIS 1.0 distingue tra operatori di servizi essenziali e fornitori di servizi digitali e gli Stati membri hanno un'ampia discrezione nel definire queste entità. Il NIS 2.0 distingue tra strutture essenziali e importanti e stabilisce un unico criterio sotto forma di una soglia per le dimensioni delle strutture.
- Nel NIS 1.0, la portata delle misure di gestione del rischio di cybersecurity richieste è vaga. Gli Stati membri hanno un ampio margine di discrezione. Il NIS 2.0 fornisce maggiori dettagli e pone una maggiore attenzione sui rischi della catena di approvvigionamento.
- Nel NIS 1.0, la portata dei requisiti di segnalazione è vaga. Il NIS 2.0 fornisce regole più chiare su quali, quando e come gli incidenti informatici devono essere segnalati. Introduce un obbligo di segnalazione per le minacce informatiche.

Motivazione della Commissione sulla sussidiarietà

L'intervento dell'UE è giustificato dalla natura transfrontaliera delle minacce legate ai NIS.

Contesto politico

Il NIS 2.0 integra la Proposta di Direttiva sulla resilienza dei soggetti critici [COM(2020) 829].

Stato della legislazione

16.12.2020	Adozione da parte della Commissione
Da definire	Adozione da parte del Parlamento europeo e del Consiglio, pubblicazione nella Gazzetta ufficiale, entrata in vigore

Referenti per influenzare il processo politico

Direzioni generali:	DG Reti di comunicazione, contenuti e tecnologie
Commissioni del Parlamento Europeo:	ITRE (referente), relatrice: Angelika Niebler (PPE, DE)
Processo decisionale nel Consiglio:	Maggioranza qualificata (approvazione del 55% degli Stati membri che rappresentano il 65% della popolazione dell'UE)

Formalità

Norme di riferimento:	Art. 114 TFUE (Mercato interno)
Natura della competenza legislativa:	Competenza concorrente (Art. 4 (2) TFUE)
Procedura:	Art. 294 TFUE (procedura legislativa ordinaria)

VALUTAZIONE

Valutazione di impatto economico

Stabilire requisiti di sicurezza informatica per le imprese centrali per il funzionamento di una società risulta appropriato: le aziende hanno già un interesse proprio a proteggere la loro rete e i loro sistemi informativi (NIS) da incidenti e minacce cibernetiche, poiché il mancato rispetto di questa regola può comportare per loro una significativa perdita di entrate e danni alla propria reputazione. Anche se comportano costi significativi e limitano la libertà delle imprese, delle misure generali comuni di tipo tecnico e organizzativo da parte dell'UE sui NIS sono comunque giustificate, anche perché **gli stimoli relativi ai costi legati alla sicurezza informatica sono ancora insufficienti**. Ciò si deve innanzitutto al fatto che le aziende spesso non devono sostenere da sole tutti i costi degli incidenti informatici, **e** possono trasferire alcuni dei costi a terzi, ad es. ai loro clienti. In secondo luogo, le aziende potrebbero beneficiare degli investimenti in cibersicurezza di altre aziende, poiché questi investimenti spesso aumentano non solo la resilienza NIS dell'investitore, ma anche indirettamente la resilienza di terzi. Inoltre, **i costi**

per la società degli incidenti informatici che colpiscono imprese essenziali e importanti sono particolarmente elevati.

A differenza della NIS 1.0, la ricalibratura del campo di applicazione della Direttiva migliora la chiarezza giuridica, limita azioni di arbitraggio normativo e quindi le distorsioni della concorrenza. Tuttavia, l'ambito di applicazione è troppo ampio: esso include molte aziende che non forniscono prodotti o servizi centrali per il funzionamento di una società, ad es. i produttori di automobili, che dovrebbero quindi essere esclusi. Inoltre, è discutibile se le autorità competenti sarebbero in grado di supervisionare adeguatamente tutte le imprese coperte dalla Direttiva - ad es. tutti i produttori di beni, vale a dire 31.000 medie e grandi imprese [SWD(2020) 345, pagina 63]. Poi la dimensione come unico criterio è inappropriata anche perché questa da sola non indica necessariamente un rischio di cibersicurezza più elevato. Dovrebbero essere presi in considerazione anche altri criteri come, ad esempio, il numero di clienti.

I nuovi obblighi per le aziende essenziali e importanti di considerare pure i rischi della catena di approvvigionamento come parte della loro gestione del rischio, in misura maggiore rispetto al NIS 1.0, possono aumentare il livello di sicurezza informatica nell'UE. Tuttavia, tali obblighi **dovrebbero essere limitati ai rischi che riguardano i fornitori di prodotti e servizi ICT considerati rilevanti per la sicurezza del business delle aziende**. L'onere non dovrebbe ricadere solo sulle aziende essenziali e importanti al termine delle catene di approvvigionamento. Ci dovrebbero essere anche requisiti per i fornitori nelle catene del valore per garantire che i loro prodotti e servizi ICT, quando forniti a società essenziali e importanti, siano sicuri dal punto di vista informatico.

Le aziende solitamente sono poco incentivate a segnalare incidenti e minacce informatiche, dati i costi di segnalazione e i potenziali danni alla reputazione. Allo stesso tempo, il *reporting* però aiuta gli altri a identificare e colmare le lacune di sicurezza. Segnalare incidenti e minacce informatiche comporta quindi significativi benefici esterni, rendendo appropriato obbligare le aziende a fare segnalazioni. **Le nuove previste procedure di segnalazione aumentano la certezza giuridica e le strutture di segnalazione centralizzate riducono l'onere amministrativo per le entità tenute alla segnalazione. L'obbligo** previsto **di segnalare gli incidenti entro 24 ore** e di fornire informazioni significative **potrebbe però rivelarsi troppo impegnativo**. Questo è particolarmente vero per le aziende più piccole. Questo obbligo di segnalazioni rapide potrebbe poi finire anche per vincolare risorse preziose presso le diverse realtà coinvolte, risorse che potrebbero essere, sul momento, meglio utilizzate per fronteggiare gli incidenti informatici.

Valutazione giuridica

Competenze

La Direttiva si basa giustamente sull'articolo 114 del TFUE. Questo vale anche per l'inclusione nel suo campo di applicazione di quelle amministrazioni pubbliche che prendono decisioni amministrative o regolamentari che riguardano le quattro libertà fondamentali. Infatti, le misure basate sull'articolo 114 del TFUE devono mirare a migliorare le condizioni per l'instaurazione e il funzionamento del mercato interno, eliminando gli ostacoli alle libertà fondamentali o eliminando le distorsioni significative della concorrenza [sentenza del 3.9.2015, C-398/13 P, Inuit Tapiriit Kanatami e altri/Commissione, EU:C:2015:535, punto 26]. Delle norme uniformi di rafforzamento della sicurezza informatica delle amministrazioni pubbliche soddisfano i criteri di cui sopra se riguardano le autorità nazionali a cui le persone fisiche e giuridiche fanno ricorso nell'esercizio dei loro diritti alla circolazione delle persone, dei beni, dei servizi o dei capitali. Questo può essere il caso, per es., quando un'autorità di vigilanza autorizza un'impresa a offrire i suoi servizi in tutto il mercato interno. In questi casi, la capacità delle amministrazioni pubbliche di svolgere i loro compiti in modo continuo e sicuro è una condizione che deve essere soddisfatta affinché le persone fisiche o giuridiche possano esercitare effettivamente questi diritti.

Sussidiarietà

Senza problemi, data la natura transfrontaliera degli incidenti e delle minacce legate alla NIS.

Proporzionalità rispetto agli Stati membri

Gli Stati membri mantengono il potere di regolamentare le misure di sicurezza informatica per le imprese non soggette alla direttiva. Mantengono anche una certa discrezionalità nel decidere l'adeguatezza e la proporzionalità delle misure tecniche e organizzative di gestione del rischio. Poiché la Direttiva prevede un'armonizzazione minima [Art. 3], gli Stati membri possono stabilire requisiti che operano su un livello più alto di sicurezza informatica.

Conclusione

I requisiti di sicurezza informatica per le imprese centrali per il funzionamento di una società sono appropriati, perché gli stimoli economici per investire nella sicurezza informatica sono insufficienti e i costi per la società sono particolarmente elevati per gli incidenti informatici che colpiscono le imprese essenziali e importanti. I nuovi obblighi per le imprese essenziali e importanti di considerare i rischi della catena di approvvigionamento dovrebbero essere limitati ai rischi che colpiscono i fornitori di prodotti e servizi ICT che sono considerati rilevanti per la sicurezza del business delle imprese. Le nuove procedure di segnalazione aumentano la chiarezza giuridica e le strutture di segnalazione centralizzate riducono l'onere amministrativo per le entità che effettuano le segnalazioni. L'obbligo di segnalare gli incidenti entro 24 ore può rivelarsi troppo impegnativo.

Autori: Philipp Eckhardt e Dr. Martina Anzini | Telefon + 49 761 38693-107| eckhardt@cep.eu
Traduzione in italiano: Prof. Andrea De Petris