COMMISSIONE
EUROPEA

Bruxelles, 13.9.2017
C(2017) 6100 final

RACCOMANDAZIONE DELLA COMMISSIONE

del 13.9.2017

relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala

RACCOMANDAZIONE DELLA COMMISSIONE

del 13.9.2017

relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 292,

considerando quanto segue:

(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica, dato che imprese e cittadini dell'Unione sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero. Un incidente di cibersicurezza che interessa le organizzazioni di più Stati membri o addirittura l'intera Unione, con potenziali gravi perturbazioni del mercato interno e più in generale delle reti e dei sistemi informativi dai quali dipendono l'economia, la democrazia e la società dell'Unione, è uno scenario per il quale gli Stati membri e le istituzioni dell'UE devono essere ben preparati.

(2) Un incidente di cibersicurezza può essere considerato una crisi a livello di Unione quando le conseguenti perturbazioni sono talmente ampie da non poter essere gestite autonomamente dallo Stato membro interessato o quando interessa due o più Stati membri e ha un impatto di rilevanza tecnica o politica di così vasta portata da richiedere un coordinamento e una risposta tempestivi a livello politico dell'Unione.

(3) Gli incidenti di cibersicurezza possono innescare crisi più ampie, con ripercussioni su altri settori di attività al di là delle reti e dei sistemi informativi e delle reti di comunicazione; per reagire adeguatamente è necessario intervenire con attività di attenuazione concernenti sia l'ambito informatico che altri ambiti.

(4) Gli incidenti di cibersicurezza sono imprevedibili e spesso si verificano ed evolvono in tempi molto ridotti, pertanto i soggetti colpiti e coloro che hanno la responsabilità di reagire e di attenuare gli effetti conseguenti devono coordinare la loro risposta rapidamente. Inoltre, spesso tali incidenti non sono circoscritti a una determinata area geografica e possono verificarsi simultaneamente o diffondersi all'istante in molti paesi.

(5) Una risposta efficace agli incidenti e alle crisi di cibersicurezza su vasta scala a livello dell'UE richiede una cooperazione rapida ed efficace tra tutti i portatori di interesse e dipende dalla preparazione e dalle capacità dei singoli Stati membri, come pure da un'azione comune coordinata sostenuta dalle capacità dell'Unione. Per rispondere in modo tempestivo ed efficace agli incidenti sono pertanto necessari procedure e meccanismi di cooperazione stabiliti in precedenza e, per quanto possibile, ben collaudati che definiscano con chiarezza i ruoli e le responsabilità dei principali attori a livello nazionale e di Unione.

(6) Nelle sue conclusioni[1] sulla protezione delle infrastrutture critiche informatizzate del 27 maggio 2011 il Consiglio ha invitato gli Stati membri dell'UE a "rafforzare la collaborazione tra gli Stati membri e contribuire, sulla base di esperienze e risultati nazionali in materia di gestione delle crisi e in collaborazione con l'ENISA, a sviluppare i meccanismi di una cooperazione europea in materia di incidenti informatici, da saggiare nel contesto della prossima esercitazione "Europa informatica" nel 2012".

(7) Nella sua comunicazione del 2016 dal titolo "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza"[2] la Commissione ha incoraggiato gli Stati membri a sfruttare al massimo i meccanismi di cooperazione della direttiva sulla sicurezza delle reti e dell'informazione (direttiva NIS)[3], come pure a rafforzare la cooperazione transfrontaliera per poter fronteggiare un incidente cibernetico su vasta scala. Ha inoltre aggiunto che la capacità di fronteggiare gli incidenti informatici su vasta scala trarrebbe vantaggio da un approccio coordinato alla cooperazione tra i vari elementi dell'ecosistema cibernetico nelle situazioni di crisi; tale approccio dovrebbe essere definito in un "programma" e dovrebbe anche garantire sinergie e coerenza con i meccanismi esistenti di gestione delle crisi.

(8) Nelle conclusioni del Consiglio[4] sulla comunicazione di cui sopra gli Stati membri hanno invitato la Commissione a presentare un tale programma da sottoporre alla valutazione degli organismi e delle altre parti interessate. La direttiva NIS tuttavia non prevede un quadro di cooperazione dell'Unione in caso di incidenti e crisi di cibersicurezza su vasta scala.

(9) La Commissione ha consultato gli Stati membri in due distinti seminari di consultazione, svoltisi a Bruxelles il 5 aprile e il 4 luglio 2017, ai quali hanno partecipato rappresentanti degli Stati membri dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), del gruppo di cooperazione istituito dalla direttiva NIS e del Gruppo orizzontale del Consiglio per le questioni riguardanti il ciberspazio, nonché rappresentanti del Servizio europeo per l'azione esterna (SEAE), dell'ENISA, di Europol/EC3 e del Segretariato generale del Consiglio (SGC).

(10) Il programma per una risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala a livello dell'Unione, riportato nell'allegato della presente raccomandazione, è il risultato delle consultazioni di cui sopra e integra la comunicazione "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza".

(11) Il programma descrive e definisce gli obiettivi e le modalità della cooperazione tra gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'UE (di seguito "istituzioni dell'UE") in risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, indicando altresì in che modo i meccanismi esistenti di gestione delle crisi possono fare pieno ricorso ai soggetti esistenti a livello dell'UE incaricati della cibersicurezza.

---

1 Conclusioni del Consiglio sulla comunicazione dal titolo "Protezione delle infrastrutture critiche informatizzate - Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale", documento 10299/11, Bruxelles, 27 maggio 2011.

2 COM(2016) 410 final del 5 luglio 2016.

3 Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dell'informazione ("direttiva NIS") recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

4 Documento 14540/16, 15 novembre 2016.

(12) Nel rispondere a una crisi di cibersicurezza ai sensi del considerando 2, il coordinamento della risposta a livello politico dell'Unione in seno al Consiglio si avvarrà dei dispositivi integrati per la risposta politica alle crisi (IPCR)[5]; la Commissione farà ricorso al processo di coordinamento delle crisi transettoriale ad alto livello del sistema ARGUS[6]. Per le crisi che presentano un'importante dimensione esterna o una forte correlazione con la politica di sicurezza e di difesa comune (PSDC) sarà attivato il meccanismo di risposta alle crisi[7] del Servizio europeo per l'azione esterna (SEAE).

(13) In alcuni settori i meccanismi di gestione delle crisi settoriali a livello di UE prevedono la cooperazione in caso di incidenti o crisi di cibersicurezza. Ad esempio, nel quadro del sistema globale di navigazione satellitare (GNSS), la decisione 2014/496/PESC del Consiglio, del 22 luglio 2014, sugli aspetti del dispiegamento, del funzionamento e dell'utilizzo del sistema globale di navigazione via satellite europeo che hanno incidenza sulla sicurezza dell'Unione europea, già definisce i rispettivi ruoli del Consiglio, dell'Alto rappresentante, della Commissione, dell'Agenzia del GNSS europeo e degli Stati membri nell'ambito della catena di responsabilità operative definite per reagire a una minaccia per l'Unione, gli Stati membri o il GNSS, anche in caso di attacchi cibernetici. La presente raccomandazione pertanto non dovrebbe lasciare impregiudicati tali meccanismi.

(14) Gli Stati membri hanno la responsabilità primaria di reagire in caso di incidenti o crisi di cibersicurezza su vasta scala che li riguardino. La Commissione, l'Alto rappresentante e le altre istituzioni o gli altri servizi dell'UE hanno tuttavia un ruolo importante, derivante dal diritto dell'Unione o dal fatto che gli incidenti e le crisi di cibersicurezza possono avere ripercussioni su tutti i settori dell'attività economica nell'ambito del mercato unico, sulla sicurezza e sulle relazioni internazionali dell'Unione e sulle istituzioni stesse.

(15) A livello di Unione, i principali soggetti coinvolti nella risposta alle crisi di cibersicurezza comprendono le strutture e i meccanismi previsti dalla direttiva NIS recentemente istituiti, vale a dire la rete dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), come pure le agenzie e gli organismi competenti, ossia l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), il Centro europeo per la lotta alla criminalità informatica di Europol (Europol/EC3), il Centro dell'UE di analisi dell'intelligence (INTCEN), la direzione di intelligence dello Stato maggiore dell'Unione europea (EUMS INT) e la sala situazione (SITROOM) che collaborano come capacità unica di analisi dell'intelligence (SIAC), la cellula dell'UE per l'analisi delle minacce ibride (presso l'INTCEN), la squadra di pronto intervento informatico delle istituzioni dell'UE (CERT-UE) e il Centro di coordinamento della risposta alle emergenze della Commissione europea.

(16) La cooperazione tra gli Stati membri per reagire agli incidenti di cibersicurezza a livello tecnico è assicurata dalla rete dei CSIRT istituita dalla direttiva NIS. L'ENISA svolge la funzione di segretariato della rete e sostiene attivamente la cooperazione fra i CSIRT. I CSIRT nazionali e il CERT-UE collaborano e si scambiano informazioni su

---

5 Ulteriori informazioni sono disponibili nella sezione 3.1. dell'appendice sulla gestione delle crisi, sui meccanismi di cooperazione e sugli attori a livello di UE.

6 Ibidem.

7 Ibidem.

base volontaria, se necessario anche in risposta a incidenti di cibersicurezza che interessano uno o più Stati membri. Su richiesta di un rappresentante del CSIRT di uno Stato membro, possono discutere e, ove possibile, individuare un intervento coordinato per un incidente rilevato nella giurisdizione dello Stato membro in questione. Le procedure pertinenti saranno definite nell'ambito delle procedure operative standard (POS) della rete dei CSIRT[8].

(17) La rete dei CSIRT ha inoltre il compito di discutere, esaminare e individuare ulteriori forme di cooperazione operativa, anche in relazione alle categorie di rischi e di incidenti, all'allerta precoce, all'assistenza reciproca, ai principi e alle modalità di coordinamento, quando gli Stati membri intervengono a proposito di rischi e incidenti transfrontalieri.

(18) Il gruppo di cooperazione istituito dall'articolo 11 della direttiva NIS ha il compito di fornire orientamenti strategici per le attività della rete dei CSIRT, di discutere della capacità e dello stato di preparazione degli Stati membri e, su base volontaria, di valutare le strategie nazionali in materia di sicurezza della rete e dei sistemi informativi e l'efficacia dei CSIRT e di individuare le migliori pratiche.

(19) Un *workstream* dedicato all'interno del gruppo di cooperazione sta elaborando orientamenti in materia di notifica degli incidenti, a norma dell'articolo 14, paragrafo 7, della direttiva NIS, concernenti i casi in cui gli operatori di servizi essenziali sono tenuti a notificare gli incidenti a norma dell'articolo 14, paragrafo 3, e il formato e la procedura di tali notifiche[9].

(20) La conoscenza e la comprensione della situazione in tempo reale, della posizione di rischio e delle minacce, acquisite attraverso relazioni, valutazioni, ricerche, indagini e analisi, sono fondamentali per poter prendere decisioni con cognizione di causa. La "conoscenza situazionale" da parte di tutte le parti interessate è essenziale per l'efficacia della risposta coordinata. La conoscenza situazionale comprende gli elementi relativi alle cause, all'impatto e all'origine dell'incidente. È risaputo che essa dipende dallo scambio e dalla condivisione di informazioni tra le parti interessate in un formato idoneo, mediante il ricorso a una tassonomia comune per la descrizione dell'incidente e secondo modalità sicure.

(21) La risposta agli incidenti di cibersicurezza può assumere molte forme, che vanno dall'individuazione di misure tecniche che possono comportare la ricerca congiunta - da parte di due o più soggetti - delle cause tecniche dell'incidente (ad esempio, analisi dei programmi malevoli, noti anche come *malware*) o l'identificazione dei modi in cui le organizzazioni possono valutare se sono state colpite (ad esempio, indicatori di compromissione) alle decisioni operative sull'applicazione di tali misure e, a livello politico, sulla scelta di ricorrere ad altri strumenti, ad esempio al quadro relativo a una risposta comune alle attività informatiche dolose[10] o al protocollo operativo dell'UE per contrastare le minacce ibride[11], in funzione dell'incidente.

---

8 In corso di elaborazione; dovrebbero essere adottate entro la fine del 2017.

9 Gli orientamenti dovrebbero essere completati entro la fine del 2017.

10 Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")", documento 9916/17.

11 Documento di lavoro dei servizi della Commissione: "EU operational protocol for countering hybrid threats 'EU Playbook'", SWD(2016) 227 final del 5.7.2016.

(22) La fiducia dei cittadini e delle imprese europei nei servizi digitali è essenziale per un mercato unico digitale fiorente. Pertanto, la comunicazione in caso di crisi riveste un ruolo particolarmente importante nell'attenuazione degli effetti negativi degli incidenti e delle crisi di cibersicurezza. La comunicazione può essere utilizzata anche nell'ambito del quadro relativo a una risposta diplomatica comune come strumento per influenzare il comportamento dei (potenziali) aggressori che agiscono da paesi terzi. L'allineamento della comunicazione pubblica per attenuare gli effetti negativi degli incidenti e delle crisi di cibersicurezza e l'uso della comunicazione pubblica per influenzare un aggressore sono essenziali per dare efficacia alla risposta politica.

(23) Informare la popolazione su come attenuare, a livello di utente e di organizzazione, gli effetti di un incidente (ad esempio mediante l'applicazione di aggiornamenti di sicurezza o il ricorso ad azioni complementari per evitare la minaccia) potrebbe essere una misura efficace per ridurre l'impatto di un incidente o di una crisi di cibersicurezza su vasta scala.

(24) La Commissione, attraverso l'infrastruttura di servizi digitali per la cibersicurezza del Meccanismo per collegare l'Europa (MCE), sta sviluppando un meccanismo di cooperazione basato su una piattaforma di servizi essenziali (noto come MeliCERTes) tra i CSIRT degli Stati membri partecipanti per migliorare il loro livello di preparazione, cooperazione e reazione alle minacce e agli incidenti cibernetici emergenti. La Commissione, mediante inviti a presentare proposte su base concorrenziale per la concessione di sovvenzioni nell'ambito dell'MCE cofinanzia i CSIRT negli Stati membri al fine di migliorare le loro capacità operative a livello nazionale.

(25) Per promuovere e migliorare la collaborazione tra Stati membri e settore privato è fondamentale organizzare esercitazioni sugli incidenti cibernetici a livello dell'UE. A tal fine, dal 2010 l'ENISA organizza regolarmente esercitazioni paneuropee sugli incidenti cibernetici (''Cyber Europe'').

(26) Nelle sue conclusioni[12] sull'attuazione della dichiarazione congiunta del Presidente del Consiglio europeo, del Presidente della Commissione europea e del Segretario generale dell'Organizzazione del trattato del Nord Atlantico, il Consiglio chiede il rafforzamento della cooperazione nelle esercitazioni di cibersicurezza attraverso la reciproca partecipazione del personale alle rispettive esercitazioni, comprese in particolare Cyber Coalition e Cyber Europe.

(27) Il panorama delle minacce in costante evoluzione e i recenti incidenti di cibersicurezza sono un'indicazione del rischio crescente cui deve far fronte l'Unione; gli Stati membri dovrebbero dar seguito alla presente raccomandazione senza ulteriore indugio e in ogni caso entro la fine del 2018,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

(1) Gli Stati membri e le istituzioni dell'UE dovrebbero istituire un quadro di risposta alle crisi di cibersicurezza dell'UE che integri gli obiettivi e le modalità di cooperazione descritti nel programma attenendosi ai principi guida ivi riportati.

(2) Il quadro di risposta alle crisi di cibersicurezza dell'UE dovrebbe in particolare individuare i soggetti interessati, le istituzioni dell'UE e le autorità degli Stati membri competenti a tutti i livelli necessari - tecnico, operativo, strategico/politico - ed

[12] ST 15283/16, 6 dicembre 2016.

elaborare, ove necessario, procedure operative standard che definiscano le modalità di cooperazione dei soggetti di cui sopra nell'ambito dei meccanismi UE di gestione delle crisi. L'accento dovrebbe essere posto sulla necessità di consentire lo scambio di informazioni senza indebiti ritardi e sul coordinamento della risposta durante gli incidenti e le crisi di cibersicurezza su vasta scala.

(3) A tal fine, le autorità competenti degli Stati membri dovrebbero collaborare per specificare ulteriormente i protocolli per la condivisione delle informazioni e la cooperazione. Il gruppo di cooperazione dovrebbe procedere allo scambio delle esperienze acquisite in materia con le competenti istituzioni dell'UE.

(4) Gli Stati membri dovrebbero provvedere affinché i meccanismi nazionali di gestione delle crisi reagiscano in modo adeguato agli incidenti di cibersicurezza e creare le procedure necessarie per la cooperazione a livello dell'UE nell'ambito del quadro dell'UE.

(5) In linea con il programma, gli Stati membri dovrebbero, in collaborazione con i servizi della Commissione e il SEAE, stabilire orientamenti per l'attuazione pratica per quanto riguarda l'integrazione delle loro procedure e dei soggetti nazionali incaricati della gestione delle crisi e della cibersicurezza nei vigenti meccanismi dell'UE di gestione delle crisi, vale a dire l'IPCR e il CRM del SEAE. In particolare, gli Stati membri dovrebbero garantire che vengano predisposte le strutture appropriate per consentire un flusso di informazioni efficiente tra le rispettive autorità nazionali di gestione delle crisi e i loro rappresentanti a livello dell'UE nell'ambito dei meccanismi UE di gestione delle crisi.

(6) Gli Stati membri dovrebbero avvalersi pienamente delle opportunità offerte dal programma delle infrastrutture di servizi digitali del Meccanismo per collegare l'Europa (MCE) e collaborare con la Commissione per garantire che il meccanismo di cooperazione della piattaforma di servizi essenziali, attualmente in corso di sviluppo, fornisca le funzionalità necessarie e soddisfi i requisiti per la cooperazione anche durante le crisi di cibersicurezza.

(7) Gli Stati membri, con l'assistenza dell'ENISA e sulla base del lavoro già svolto in questo ambito, dovrebbero cooperare all'elaborazione e all'adozione di una tassonomia e di un modello comuni per la descrizione delle cause tecniche e delle ripercussioni degli incidenti di cibersicurezza nelle relazioni sulla situazione, al fine di rafforzare ulteriormente la cooperazione tecnica e operativa durante le crisi. A tale riguardo, gli Stati membri dovrebbero tener conto dei lavori in corso nell'ambito del gruppo di cooperazione sugli orientamenti in materia di notifica degli incidenti, in particolare, degli aspetti relativi al formato delle notifiche nazionali.

(8) Le procedure stabilite nel quadro dovrebbero essere provate e, se necessario, rivedute a seguito degli insegnamenti tratti dalla partecipazione degli Stati membri alle esercitazioni di cibersicurezza a livello nazionale, regionali, dell'Unione e della NATO, nonché nell'ambito della diplomazia cibernetica. Dovrebbero essere provate in particolare nel quadro delle esercitazioni Cyber Europe organizzate dall'ENISA. Cyber Europe 2018 offre per la prima volta questa opportunità.

(9) Gli Stati membri e le istituzioni dell'UE dovrebbero organizzare regolarmente esercitazioni per verificare la loro risposta agli incidenti e alle crisi di cibersicurezza su vasta scala a livello nazionale ed europeo, anche per quanto riguarda la risposta politica, se del caso coinvolgendo soggetti del settore privato.

Fatto a Bruxelles, il 13.9.2017

Per la Commissione
Mariya GABRIEL
Membro della Commissione

PER COPIA CONFORME
Per il Segretario generale

Jordi AYET PUIGARNAU
Direttore della cancelleria
COMMISSIONE EUROPEA