Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione

VERSO UNA CULTURA DELLA SICUREZZA

ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO

ORGANIZZZIONE PER LA COOPERAZIONE E LO SVILIUPPO ECONOMICO

In virtù dell'art.1 della Convenzione firmata il 14 dicembre 1960 ed entrata in vigore il 30 settembre 1961, l'Organizzazione per la Cooperazione e lo Sviluppo Economici (OCSE) ha per obiettivo di favorire le politiche tese a:

- realizzare la maggiore espansione possibile dell'economia e dell'occupazione ed un innalzamento del livello di vita nei Paesi Membri, pur mantenendo la stabilità finanziaria, e di contribuire così allo sviluppo dell'economia mondiale;
- contribuire a una sana espansione economica nei Paesi Membri, e non membri, in via di sviluppo economico;
- contribuire all'espansione del commercio mondiale su una base multilaterale e non discriminatoria, in conformità agli impegni internazionali.

I Membri fondatori dell'OCSE sono: Austria, Belgio, Canada, Danimarca, Francia, Germania, Grecia, Irlanda, Islanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Portogallo, Regno Unito, Spagna, Stati Uniti, Svezia, Svizzera, Turchia. I seguenti paesi sono in seguito diventati Membri per adesione alle date di seguito indicate: Giappone (28 aprile 1964), Finlandia (28 gennaio 1969), Australia (7 giugno 1971), Nuova Zelanda (29 maggio 1973), Messico (18 maggio 1994), Repubblica Ceca (21 dicembre 1995), Ungheria (7 maggio 1996), Polonia (22 novembre 1996) e Corea (12 dicembre 1996). La Commissione delle Comunità Europee partecipa ai lavori dell'OCSE (art.13 della Convenzione dell'OCSE).

Also available in English under the title:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

PREMESSA

Le presenti *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione: verso una cultura della sicurezza* sono state adottate sotto forma di Raccomandazione del Consiglio in occasione della 1037ª sessione del Consiglio dell'OCSE, il 25 luglio 2002.

INDICE

LINEE GUIDA SULLA SICUREZZA DEI SISTEMI E DELLE RETI D'INFORMAZIONE:
VERSO UNA CULTURA DELLA SICUREZZA..... 7

PREFAZIONE 7

I. VERSO UNA CULTURA DELLA SICUREZZA 8

II. OBIETTIVI..... 8

III. PRINCIPI..... 9

RACCOMANDAZIONE DEL CONSIGLIO 15

ITER DELLA PROCEDURA 18

LE LINEE GUIDA SULLA SICUREZZA DEI SISTEMI E DELLE RETI D'INFORMAZIONE

VERSO UNA CULTURA DELLA SICUREZZA

PREFAZIONE

L'uso dei sistemi e delle reti d'informazione e l'ambiente delle tecnologie dell'informazione nel suo insieme, hanno registrato spettacolari cambiamenti dal 1992, data della prima pubblicazione delle *Linee guida sulla sicurezza dei sistemi e reti d'informazione* dell'OCSE. Tali continui cambiamenti offrono notevoli vantaggi ma richiedono altresì che i governi, le imprese, le altre istituzioni e i singoli utenti che sviluppano, possiedono, forniscono, gestiscono, procedono alla manutenzione e utilizzano i sistemi e le reti d'informazione (parti interessate), dedichino maggiore attenzione alla sicurezza.

Personal computer sempre più potenti, tecnologie convergenti e un'ampia utilizzazione d'Internet hanno sostituito i precedenti sistemi autonomi dalle capacità limitate nell'ambito di reti prevalentemente chiuse. Oggi, le parti interessate sono sempre più interconnesse e le connessioni superano i confini nazionali. Inoltre, Internet è il supporto per infrastrutture vitali quali l'energia, i trasporti e le attività finanziarie e svolge un ruolo centrale nel modo in cui le imprese svolgono le proprie attività, in cui i governi assicurano i servizi ai cittadini e alle imprese e in cui i cittadini comunicano e scambiano informazioni. La natura e la tipologia delle tecnologie che costituiscono l'infrastruttura delle comunicazioni e dell'informazione hanno parimenti registrato una notevole evoluzione. Il numero e la natura dei dispositivi di accesso a tale infrastruttura si sono moltiplicati e differenziati per conglobare i terminali di accesso fissi, senza fili e mobili e gli accessi tramite collegamenti "permanenti" sono in aumento. Ne consegue che la natura, il volume e il carattere sensibile dell'informazione scambiata sono aumentati in modo sostanziale.

Con la loro accresciuta connettività, i sistemi e reti d'informazione sono ormai esposti a un aumento del numero e a una più larga gamma di minacce e vulnerabilità ed emergono quindi nuovi problemi di sicurezza. Per tale motivo, le presenti Linee guida non sono rivolte all'insieme delle parti interessate nell'ambito della nuova società dell'informazione, e suggeriscono la necessità di una maggiore vigilanza e comprensione riguardo alle questioni di sicurezza, e la necessità di sviluppare una "cultura della sicurezza".

I. VERSO UNA CULTURA DELLA SICUREZZA

Le presenti Linee guida rispondono a un contesto in continua evoluzione incitando allo sviluppo di una cultura della sicurezza – sottolineando quindi la necessità di dedicare la massima attenzione alla sicurezza nella fase di sviluppo dei sistemi informativi e delle reti e adottando nuovi approcci e nuovi comportamenti nell'utilizzazione dei sistemi e delle reti d'informazione e nelle interazioni realizzate mediante tali sistemi. Le Linee guida rappresentano una netta svolta rispetto a un'epoca in cui la sicurezza interveniva troppo spesso in modo saltuario nella progettazione e nell'uso delle reti e dei sistemi informativi. Le parti interessate sono sempre più dipendenti dai sistemi d'informazione, dalle reti e dai servizi a loro collegati, i quali devono essere tutti affidabili e sicuri. Solo un approccio che tenga debitamente conto degli interessi di tutte le parti e della natura dei sistemi, reti e servizi connessi, è in grado di offrire un'efficace sicurezza.

Ogni singola parte interessata ha un rilevante ruolo da svolgere per tutelare la sicurezza. Le parti interessate, secondo i loro rispettivi ruoli, devono essere sensibilizzate ai rischi legati alla sicurezza, nonché alle protezioni adeguate e devono assumere le loro responsabilità e prendere misure per migliorare la sicurezza dei sistemi e reti d'informazione.

La diffusione di una cultura della sicurezza richiederà un impulso e una larga partecipazione e dovrebbe portare a conferire una rafforzata priorità alla programmazione e alla gestione della sicurezza e a un'estensione della comprensione della necessità della sicurezza a tutte le parti interessate. Le questioni di sicurezza devono essere un argomento di preoccupazione e di responsabilità a tutti livelli di governo e, delle imprese e per l'insieme delle parti interessate. Le Linee guida offrono un punto di appoggio per instaurare una cultura della sicurezza nell'insieme della società. Le parti interessate potranno così integrare la sicurezza nella progettazione e nell'utilizzazione di tutti i sistemi e di tutte le reti d'informazione. Le Linee guida propongono che tutte le parti interessate adottino e incoraggino una "cultura della sicurezza" per orientare la riflessione, la decisione e l'azione concernenti il funzionamento dei sistemi e delle reti d'informazione.

II. FINALITA'

Lo scopo delle Linee guida è di:

- Estendere all’insieme delle parti interessate una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti d’informazione.
- Rafforzare la sensibilità rispetto ai rischi per i sistemi e le reti d’informazione, alle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi, nonché alla necessità di adottarli e di attuarli.
- Favorire una maggiore fiducia delle parti nei confronti dei sistemi e delle reti d’informazione e nel modo in cui sono forniti ed utilizzati.
- Creare un assetto generale di riferimento che aiuti le parti interessate a comprendere la natura dei problemi legati alla sicurezza e a rispettare i valori etici nell'elaborazione e nell'attuazione di politiche, pratiche, azioni e procedure coerenti per la sicurezza dei sistemi e reti d’informazione.
- Incoraggiare fra tutte le parti interessate, la cooperazione e la condivisione d’informazioni adeguate all'elaborazione e all'attuazione di politiche, pratiche, azioni e procedure intese alla sicurezza.
- Promuovere la presa in considerazione della sicurezza quale obiettivo rilevante per tutte le parti interessate associate all'elaborazione e all'attuazione di norme.

III. PRINCIPI

I nove principi di seguito presentati sono complementari e devono essere considerati come un insieme. Essi riguardano le parti interessate a tutti i livelli, compreso quello politico e operativo. Secondo quanto indicato dalle Linee guida, le responsabilità delle parti interessate variano secondo il ruolo da loro assunto. Tutte le parti interessate saranno assistite con interventi di sensibilizzazione, d’istruzione, di scambi d'informazione e di formazione per facilitare una migliore comprensione degli argomenti di sicurezza e l'adozione di migliori pratiche in tale settore. Gli sforzi tesi a rafforzare la sicurezza dei sistemi e delle reti d’informazione devono rispettare i valori di una società democratica, in particolare l’esigenza di una libera ed aperta circolazione

dell'informazione e i principi di base del rispetto della vita privata delle singole persone.[1]

1) Sensibilizzazione

Le parti interessate devono essere consapevoli della necessità di tutelare la sicurezza dei sistemi e delle reti d'informazione e delle azioni che possono intraprendere per rafforzare la sicurezza.

La sensibilizzazione sui rischi e sulle protezioni disponibili, è la prima linea di difesa per assicurare la sicurezza dei sistemi e delle reti d'informazione. I sistemi e le reti d'informazione possono essere sottoposti a rischi interni ed esterni. Le parti interessate non solo devono sapere che le falle in materia di sicurezza, possono gravemente incidere sull'integrità dei sistemi e delle reti che controllano ma devono essere anche consapevoli che a causa dell'interconnettività e dell'interdipendenza tra sistemi, essi possono potenzialmente danneggiare le altre parti. Le parti interessate devono riflettere alla configurazione del loro sistema, agli aggiornamenti disponibili per quest'ultimo, allo spazio occupato dal loro sistema nelle reti, alle buone pratiche che possono attuare per rafforzare la sicurezza, nonché ai bisogni delle altre parti interessate.

2) Responsabilità

Le parti interessate sono responsabili della sicurezza dei sistemi e delle reti d'informazione.

Le parti interessate dipendono da sistemi e da reti d'informazione locali e globali interconnessi. Esse devono essere consapevoli della loro responsabilità rispetto alla sicurezza di tali sistemi e reti ed esserne individualmente responsabili in funzione del loro ruolo. Esse devono regolarmente esaminare e valutare le proprie politiche, pratiche, misure e procedure per verificare se siano adeguate al loro ambiente. Coloro che sviluppano, progettano e forniscono prodotti e servizi devono rispondere all'esigenza di sicurezza dei sistemi e delle reti e diffondere informazioni

1. In aggiunta alle presenti Linee guida sulla sicurezza, l'OCSE ha elaborato una serie di raccomandazioni integrative concernenti altri aspetti rilevanti della società globale dell'informazione. Esse riguardano la sfera privata (Linee guida sulla tutela della vita privata e i flussi transfrontalieri di dati a carattere personale, OCSE 1980) e la crittografia (Linee guida per la tutela della politica di crittografia, OCSE, 1997). Le presenti Linee guida sulla sicurezza devono essere lette insieme con le Linee guida menzionate più sopra.

adeguate, in particolare tempestivi aggiornamenti affinché gli utenti siano in grado di comprendere meglio le funzioni di sicurezza dei prodotti e dei servizi e le loro responsabilità in materia.

3) Risposta

Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.

A causa dell'interconnettività dei sistemi e delle reti d'informazione e della tendenza mostrata dai danni a diffondersi, rapidamente ed in modo molto esteso, le parti interessate devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione. Esse devono scambiare, in maniera adeguata, le informazioni di cui dispongono sulle minacce e vulnerabilità e devono creare procedure per una rapida ed efficace cooperazione volta a prevenire e a rilevare gli incidenti di sicurezza e a rispondervi. Ciò potrebbe comportare scambi d'informazioni e una cooperazione transfrontaliera, ove autorizzato.

4) Etica

Le parti interessate devono rispettare i legittimi interessi delle altre parti.

I sistemi e le reti d'informazione sono presenti ovunque nelle nostre società e, le parti interessate debbano essere consapevoli del fatto che la loro azione o inazione può causare danni ad altrui. Un comportamento etico è quindi indispensabile e le parti interessate devono adoperarsi per elaborare e adottare pratiche esemplari e incoraggiare comportamenti che tengano conto degli imperativi di sicurezza e che rispettino gli interessi legittimi delle altre parti interessate.

5) Democrazia

La sicurezza dei sistemi e delle reti d'informazione deve essere compatibile con i valori fondamentali di una società democratica.

La sicurezza deve essere assicurata nel rispetto dei valori riconosciuti dalle società democratiche e, in particolare la libertà di scambiare pensieri e idee, della circolazione dell'informazione, la riservatezza dell'informazione e delle comunicazioni, la riservatezza delle informazioni a carattere personale, l'apertura e la trasparenza.

6) Valutazione dei rischi

Le parti interessate devono procedere a valutazioni dei rischi.

La valutazione dei rischi consente d'individuare le minacce e le vulnerabilità e deve essere sufficientemente estesa per coprire l'insieme dei principali fattori interni ed esterni quali la tecnologia, i fattori fisici e umani, le politiche e i servizi forniti da terzi che hanno implicazioni sulla sicurezza. La valutazione dei rischi consentirà di determinare il livello accettabile di rischio e, faciliterà l'istituzione di misure di controllo adeguate per gestire il rischio di pregiudizio per i sistemi e le reti d'informazione secondo la natura e il valore dell'informazione da proteggere. La valutazione dei rischi deve tenere conto dei pregiudizi sugli interessi altrui o causati ad altrui, resi possibili dalla sempre più estesa interconnessione dei sistemi informativi.

7) Concezione e applicazione della sicurezza

Le parti interessate devono integrare la sicurezza quale elemento essenziale dei sistemi e delle reti d'informazione.

I sistemi, le reti e le politiche devono essere adeguatamente concepiti, applicati e coordinati per massimizzare la sicurezza. Uno degli assi più importanti, ma non esclusivo, di tale sforzo si concentra sulla concezione e sull'adozione di misure di protezione e delle soluzioni adeguate per prevenire o limitare i possibili pregiudizi legati alle vulnerabilità e alle minacce identificate. Le misure di protezione e le soluzioni devono essere allo stesso tempo, tecniche e non tecniche e commisurate al valore dell'informazione nei sistemi e reti d'informazione dell'organizzazione. La sicurezza deve essere un elemento fondamentale dell'insieme dei prodotti, servizi, sistemi e reti e deve far parte integrante della concezione e dell'architettura dei sistemi. Per l'utente finale, la concezione e l'attuazione della sicurezza servono essenzialmente a selezionare e configurare prodotti e servizi per i propri sistemi.

8) Gestione della sicurezza

Le parti interessate devono adottare un approccio globale della gestione della sicurezza.

La gestione della sicurezza deve essere basata sulla valutazione dei rischi ed essere dinamica e globale, per coprire tutti i livelli di attività delle parti interessate e tutti gli aspetti dei loro interventi. Essa deve altresì anticipare e includere le risposte alle minacce emergenti, la prevenzione, la rilevazione e la soluzione agli incidenti, la riattivazione dei sistemi, la

manutenzione permanente, il controllo et l'audit. Le politiche di sicurezza dei sistemi e delle reti d'informazione, le pratiche, le azioni e le procedure in materia di sicurezza devono essere coordinate ed integrate per creare un coerente sistema di sicurezza.

9) Rivalutazione

Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti di informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e le procedure di sicurezza.

Nuove o mutevoli vulnerabilità e minacce sono costantemente scoperte. Tutte le parti interessate devono permanentemente riesaminare, rivalutare e modificare tutti gli aspetti della sicurezza per affrontare tali rischi evolutivi.

RACCOMANDAZIONE DEL CONSIGLIO CONCERNENTE LE LINEE GUIDA SULLA SICUREZZA DEI SISTEMI E DELLE RETI D'INFORMAZIONE

VERSO UNA CULTURA DELLA SICUREZZA

Il CONSIGLIO,

Vista la Convenzione relativa all'Organizzazione per la Cooperazione e lo Sviluppo Economico del 14 dicembre 1960 e in particolare, visti i suoi articoli 1 b), 1 c), 3 a) et 5 b) ;

Vista la Raccomandazione del Consiglio concernente le Linee guida sulla protezione della vita privata e su i flussi transfrontalieri di dati di carattere personale, del 23 settembre 1980 [C(80)58(Final)] ;

Vista la Dichiarazione su i flussi transfrontalieri di dati adottata dai governi dei Paesi membri dell'OCSE, dell'11 aprile 1985 [C(85)139, Allegato] ;

Vista la Raccomandazione del Consiglio relativa alle Linee guida sulla politica di crittografia, del 27 marzo 1997 [C(97)62/FINAL] ;

Vista la Dichiarazione ministeriale relativa alla protezione della vita privata sulla rete mondiale, del 7-9 dicembre 1998 [C(98)177/FINAL, Allegato] ;

Vista la Dichiarazione ministeriale sull'autenticazione per il commercio elettronico, del 7-9 dicembre 1998 [C(98)177/FINAL, Allegato] ;

Riconoscendo che i sistemi e le reti d'informazione sono sempre più adoperati e acquisiscono una crescente valenza per i governi, le imprese, le altre organizzazioni e i singoli utenti;

Riconoscendo che il crescente ruolo svolto dai sistemi e dalle reti d'informazione nella stabilità e l'efficienza delle economie nazionali e degli scambi internazionali, e nella vita sociale, culturale e politica, e l'accentuarsi della dipendenza nei loro confronti impongono particolari sforzi per proteggere e favorire la fiducia nei loro confronti;

Riconoscendo che i sistemi e le reti d'informazione e il loro espandersi al livello mondiale conducono a nuovi e ad accresciuti rischi;

Riconoscendo che i dati e le informazioni conservati o trasmessi per il tramite di reti d'informazione, sono esposti a minacce dovute ai vari mezzi che consentono di accedere senza permesso, all'utilizzazione, all'illecita appropriazione, all'alterazione, alla trasmissione di codici malevoli, al rifiuto di servizio o alla distruzione, e richiedono adeguate misure di protezione;

Riconoscendo la necessità di un'ulteriore sensibilizzazione su i rischi che incidono su i sistemi e sulle reti d'informazione e sulle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi e di incoraggiare adeguati comportamenti in quanto costituiscono una tappa essenziale nello sviluppo di una cultura della sicurezza ;

Riconoscendo la necessità di rivedere le politiche, le pratiche, azioni e procedure attuali per adoperarsi affinché rispondano adeguatamente alle sfide in continuo mutamento, poste dalle minacce alle quali sono esposti i sistemi e le reti d'informazione ;

Riconoscendo il comune interesse a incoraggiare la sicurezza dei sistemi e delle reti d'informazione mediante una cultura della sicurezza che incoraggi un coordinamento e una cooperazione internazionale adeguati, per rispondere alle sfide poste dai pregiudizi che le falle di sicurezza possono causare alle economie nazionali, agli scambi internazionali, nonché alla partecipazione alla vita sociale, culturale e politica.

Riconoscendo inoltre che le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza*, allegate alla presente Raccomandazione, sono di applicazione volontaria e non incidono sui diritti sovrani degli Stati ;

E riconoscendo che lo scopo delle presenti Linee guida, non è quello di suggerire che esiste una qualsiasi e unica soluzione in materia di sicurezza, né tantomeno d'indicare quali politiche, pratiche, azioni e procedure particolari siano adeguate ad una data situazione, quanto di fornire un assetto più generale di principi che sia in grado di favorire una migliore comprensione sul modo in cui le parti interessate, possono allo stesso tempo usufruire dello sviluppo di una cultura della sicurezza e contribuirvi;

PRECONIZZA l'attuazione delle presenti *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza* dai governi, dalle imprese, dalle altre organizzazioni e dai singoli utenti che sviluppano, possiedono, forniscono, gestiscono, procedono alla manutenzione e utilizzano sistemi e reti d'informazione;

RACCOMANDA ai Paesi Membri :

Di elaborare nuove politiche, pratiche, azioni e procedure o di modificare quelle esistenti per rispecchiare e prendere in conto le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza,* adottando e favorendo una cultura della sicurezza, conformemente alle predette Linee guida;

Di avviare azioni di consultazione, di coordinamento e di cooperazione, a livello nazionale e internazionale, per l'applicazione delle Linee guida;

Di diffondere le Linee guida nell'insieme dei settori, pubblico e privato, in particolare presso i governi, le imprese, le altre organizzazioni e i singoli utenti, per diffondere una cultura della sicurezza, e incoraggiare tutte le parti interessate a adottare un comportamento responsabile e a adottare le necessarie misure secondo il ruolo che svolgono ;

Di mettere le Linee guida alla disposizione dei Paesi non membri il più rapidamente possibile e in maniera adeguata ;

Di procedere ogni cinque anni al riesame delle Linee guida al fine di promuovere una cooperazione internazionale sulle questioni connesse alla sicurezza dei sistemi e delle reti d'informazione ;

INCARICA il Comitato della politica dell'informazione, dell'informatica e delle comunicazioni dell'OCSE di fornire il suo sostegno all'applicazione delle Linee guida.

La presente Raccomandazione sostituisce la Raccomandazione del Consiglio sulle Linee guida per la sicurezza dei sistemi d'informazione del 26 novembre 1992 [C(92)188/FINAL].

ITER DELLA PROCEDURA

Le Linee guida sulla sicurezza sono state ultimate nel 1992 e quindi riesaminate nel 1997. Il presente esame è stato avviato nel 2001 dal Gruppo di lavoro sulla sicurezza dell'informazione e la vita privata (GLSIFP), nell'ambito di un mandato attribuito dal Comitato della Politica dell'informazione, dell'informatica e delle comunicazioni (PIIC) e accelerato a seguito della tragedia dell'11 settembre.

La stesura è stata avviata da un Gruppo di esperti del GLSIFP riunitosi a Washington, DC, il 10 e 11 dicembre 2001, a Sydney il 12-13 febbraio 2002 e a Parigi il 4-6 marzo 2002. Il GLSIFP si è riunito il 5-6 marzo 2002, il 22-23 aprile 2002 e il 25-26 giugno 2002.

Le presenti *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza* sono state adottate sotto forma di Raccomandazione del Consiglio dell'OCSE nella sua 1037ª sessione, il 25 luglio 2002.