Cybersecurity

Milano, 15 Giugno 2023

Dott. Pietro Ostuni

Cybersecurity

La ***cybersicurezza*** è definita come

"l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"

Regolamento UE 2019/881

I recenti cyber attack in Italia

il Giornale

DAL 1974 CONTRO IL CORO

ATTACCO INFORMATICO

Gli hacker russi: «Guerra all'Italia»

La minaccia dei pirati del web: colpo irreparabile Zelensky a Kharkiv, rimosso il capo della sicurezza

Ue, slitta ancora l'accordo sull'embargo al petrolio

Attorno al Pd crescono i cespugli ambientalisti

Il capolavoro di Berlusconi e Galliani: il Monza per la prima volta in Serie A

Tajani: «Nessuna divisione Tutta Fi è con il Cavaliere»

Chi boicotta Twitter e Tesla

«Io, cardinale dalla Mongolia»

Draghi vince il match della rete unica

«Con il processo Ruby ter la giustizia è ingiusta»

Servizio | Allarme sicurezza

Milano, attacco hacker agli ospedali Fatebenefratelli e Sacco

L'attacco ai server dei siti di Fatebenefratelli e Sacco ha avuto conseguenze anche su altre sedi aziendali: i presidi Buzzi e Melloni e 33 sedi territoriali

ATTACCO HACKER ALL'ASL AQUILANA: L'IRA DI PAOLUCCI, "I MAGGIORI DISAGI SI AVVERTONO NEL CHIETINO"

17 Maggio 2023 12:16

CHIETI - SANITÀ

L’obiettivo della proposta

15 settembre 2022

Commissione europea

Ha presentato

Cyber Resilience Act

Proposta di regolamento che mira a definire un ampio quadro normativo per la sicurezza informatica dei prodotti digitali connessi in rete (*“Internet of Things”*) ed immessi sul mercato dell’Unione, prevedendo obblighi più stringenti in capo ai relativi produttori

*Con il Regolamento, la **Commissione Europea** intende definire degli standard comuni di sicurezza informatica per i prodotti digitali connessi in rete (cd. “IoT”) e per i relativi servizi.*

L’obiettivo principale è quello di proteggere i consumatori e il mercato dagli incidenti informatici, salvaguardando le imprese e gli utenti che acquistano o utilizzano prodotti, o software, con componenti digitali

La strategia europea in materia di cybersecurity

Per contrastare **i crescenti costi della sicurezza informatica** ed affrontare le relative **vulnerabilità**, la Commissione si prefigge di perseguire quattro specifici obiettivi:

creare un **quadro comune europeo per la *cybersecurity* nella UE**

garantire che i produttori migliorino la sicurezza informatica dei prodotti, sin dalla fase di progettazione e durante l'intero ciclo di vita

aumentare la trasparenza delle pratiche di sicurezza informatica e delle proprietà tecniche dei prodotti

fornire ai consumatori e alle aziende prodotti sicuri pronti all'utilizzo

Le regole per i produttori

A quali prodotti si applica?

Il Regolamento si applica a qualunque prodotto *software* o *hardware*, incluse le relative soluzioni di elaborazione dati a distanza se essenziali all'operatività del prodotto, durante l'intero ciclo di vita dello stesso, dalla fase di progettazione fino alla fase di obsolescenza. **In buona sostanza, esso coprirà sia i prodotti digitali fisici, come i dispositivi IoT, sia i prodotti digitali immateriali, come i prodotti *software* incorporati nei dispositivi connessi**

Le regole per i produttori

Cosa devono fare i produttori?

- ✓ **sui produttori incombe l'onere di appurare e, conseguentemente, dichiarare che i prodotti con elementi digitali dispongano di un marchio di conformità UE**, come previsto all'art. 20 del Regolamento, mentre sui distributori l'onere di immettere in commercio solo quei prodotti che ne sono conformi

- ✓ si **estendono gli obblighi anche alle modifiche sostanziali che intervengono nel tempo**, come ad esempio in caso di **aggiornamenti o di riparazioni del software**, o ancora di **manutenzione fisica**, prevedendo l'onere di una nuova attività di valutazione qualora dette modifiche influiscano sulla conformità del prodotto al Regolamento

- ✓ il produttore ha inoltre l'obbligo di assolvere nei confronti degli utenti obblighi minimi di natura informativa, in cui rientra **la fornitura di una esaustiva documentazione tecnica relativa al prodotto**, comprensiva della dichiarazione europea di conformità del prodotto (vi è un allegato alla norma che elenca i **contenuti minimi della documentazione tecnica** da allegare al prodotto

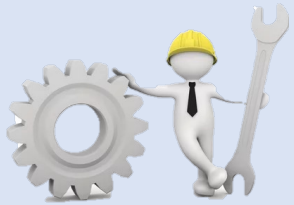
- ✓ il produttore è tenuto a garantire la conformità e la sicurezza del **per tutto il lifetime del prodotto**, con oneri di notificazione e di reportistica di informazioni concernenti incidenti e vulnerabilità del prodotto

- ✓ infine, per garantire le proprietà di sicurezza dei prodotti **gli allegati I e II alla proposta enucleano quali requisiti i manufacturers sono tenuti ad osservare** gestire correttamente le eventuali vulnerabilità rilevate, nonché quali elementi informativi minimi sono tenuti a fornire agli utenti (**l'allegato III** individua quali prodotti con elementi digitali sono classificati come "critici" in relazione all'impatto che potrebbero avere, ove sfruttate, le potenziali vulnerabilità della sicurezza)

Esclusioni

Esulano invece dal campo di applicazione i servizi come i **Software-as-a-Service**; i prodotti sviluppati per finalità militari o di sicurezza nazionale; i dispositivi medici; i prodotti rilasciati temporaneamente solo per finalità di test i prodotti relativi all'attività di omologazione dei veicoli

Quanto ai contenuti, la proposta illustra una serie di obblighi, aventi natura tecnica e organizzativa, in capo principalmente a:



MANUFACTURERS

IMPORTERS

DISTRIBUTORS

Tra le principali disposizioni giova menzionare, in particolare, il ***cybersecurity risk assessment***, che il produttore deve condurre prima dell'immissione del prodotto sul mercato e del cui esito **deve tenere conto durante le fasi di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione del prodotto**. Invero, **per tutto il ciclo di vita del prodotto** e per **almeno cinque anni dopo l'immissione sul mercato, il produttore è tenuto a garantire la sicurezza del prodotto e l'efficace gestione delle eventuali vulnerabilità.**

La sicurezza informatica in Italia

In **Italia**, la certificazione della cybersicurezza è stata da poco attuata dal **D.lgs. n. 123/2022**, entrato in vigore lo scorso 4 settembre, che recepisce la normativa europea 881/2019

Il decreto oltre a designare l'Agenzia per la cybersicurezza nazionale ("ACN") come autorità nazionale di riferimento in materia, individua nella stessa il ruolo di regolatrice della certificazione della cybersicurezza e di vigilanza sui certificati e sulle dichiarazioni di conformità

Al fine di armonizzare le normative comunitarie in materia, il Regolamento lascia impregiudicata la validità e l'efficacia del Regolamento (UE) 2016/679 sulla protezione dei dati personali ("GDPR"): tutelare i consumatori e le organizzazioni dai rischi della sicurezza informatica significa innanzitutto proteggere i loro dati

Conclusioni

La **"Direttiva NIS"** (*oggi sottoposta a revisione con la proposta di Direttiva "NIS2"*) disciplina: **la sicurezza delle reti e dei sistemi informativi; la lotta contro la criminalità informatica; le frodi; la protezione dei minori on line; la sicurezza delle reti 5G; la resilienza dei soggetti critici e i sistemi di certificazione della cybersicurezza**

Con il recente **d.l. 21 marzo 2022, n. 21**, l'Italia, spinta dagli avvenimenti in Ucraina, ha adottato disposizioni d'urgenza in materia di **diversificazione delle dotazioni informatiche delle pubbliche amministrazioni e di riorganizzazione complessiva dei poteri speciali in materia di comunicazione elettronica a banda larga basati sulla tecnologia 5G**

La **proposta** ha ad oggetto i **prodotti "*con elementi digitali*"**, intesi come prodotti o componenti *software* e *hardware*, e nasce dall'esigenza di far fronte al basso livello di sicurezza di questi prodotti e all'insufficiente consapevolezza e accesso alle informazioni relative alle proprietà di sicurezza da parte degli utenti

L'obiettivo della proposta è dunque quello, da un lato, di garantire l'immissione nel mercato di prodotti con elementi digitali sicuri, curando tra l'altro la trasparenza delle proprietà di sicurezza, e, dall'altro lato, di sensibilizzare gli utenti nella scelta e nell'utilizzo di ***hardware* e *software*** sicuri

GRAZIE PER L'ATTENZIONE

LawDeal

Società tra avvocati Law Deal S.a.s.
P.IVA 11210800964

Via Bastioni di Porta Nuova, 21
20121 Milano
Italia

Piazza del Popolo, 18
00187 Roma
Italia

info@lawdeal.it

lawdeal@pec.it