

## ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5261 di Venerdì 21 ottobre 2022

# **È in dirittura d'arrivo la legge europea sulla resilienza agli attacchi informatici**

*Per la prima volta l'Europa ha affrontato in maniera allargata il problema della sicurezza informatica di prodotti hardware e software, durante il loro intero ciclo di vita. Questo è l'obiettivo del Cyber Resilience Act.*

L'obiettivo di questo documento legislativo è quello di garantire che prodotti, che abbiano una componente digitale e siano disponibili sul mercato europeo, siano stati progettati in maniera da ridurre, per quanto ragionevolmente possibile, le vulnerabilità ad attacchi informatici e garantire che il fabbricante sia responsabile della sicurezza informatica di questi prodotti, per l'intero ciclo di vita.

Il motivo per cui gli organi legislativi europei hanno deciso di affrontare in maniera globale questo problema è facilmente comprensibile analizzando questi dati:

- ogni 11 secondi in Europa c'è un attacco ransomware,
- gli attacchi ransomware hanno prodotto perdite stimate a 20 miliardi di euro nel 2021,
- il costo annuale del crimine informatico, in Europa, è stimato a 5,5 miliardi (trillions!) di euro nel 2021.

Questa legge impone ai fabbricanti di attuare una serie di iniziative di sicurezza informatica, in fase di pianificazione, progettazione, sviluppo, produzione, consegna e manutenzione di prodotti, con una componente informatica.

Pubblicità

<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

I fabbricanti sono obbligati a riferire agli organi preposti ogni vulnerabilità e incidente, di cui vengano a conoscenza,

Una volta venduto il prodotto, i fabbricanti devono garantire che per tutta la presumibile vita utile del prodotto, o almeno per cinque anni, le vulnerabilità dei prodotti venduti vengano messe sotto controllo e corrette tempestivamente,

Infine, devono essere fornite chiare e comprensibili istruzioni per l'uso di prodotti, a rischio di attacco informatico.

Il fatto di approvare una legge, a dimensione europea, fa sì che tutti prodotti venduti nella unione europea rispettino queste regole, offrendo agli acquirenti una garanzia uniforme, indipendentemente dal paese di produzione.

Gli elaboratori di questa disposizione legislativa ritengono che il 90% dei prodotti possa rientrare in una categoria, in cui il fabbricante provvede in forma autonoma ad attuare il processo sopra illustrato.

Altri prodotti possono cadere in una classe di criticità 1, laddove è indispensabile rispettare una norma oppure chiedere una valutazione da parte di un soggetto terzo, ed infine altri possono cadere in una classe di criticità 2, dove è obbligatoria una valutazione da parte di un soggetto terzo, circa il rispetto delle prescrizioni di legge.

Vengono offerti degli esempi di strumenti, che possono cadere nelle varie categorie.

Di particolare interesse sono ovviamente i prodotti che cadono nella classe di criticità 2, come ad esempio i sistemi operativi, i firewall industriali, le CPU, gli apparati di sicurezza informatica e via di seguito.

Rientrano invece nella categoria di autovalutazione i seguenti esempi: software di manipolazione di fotografie, word processors, speaker intelligenti, giochi informatici, hard disk e via dicendo.

Per quanto riguarda la tempistica di approvazione, si confida che nella seduta plenaria del 14 -15 dicembre 2022 la legge possa essere approvata.

Può essere elemento di particolare soddisfazione per i lettori sapere che il relatore di questa legge è l'italiano Maurizio Mensi.

**Adalberto Biasiotti**



Licenza [Creative Commons](https://creativecommons.org/licenses/by-nc-nd/4.0/)

---

[www.puntosicuro.it](http://www.puntosicuro.it)