PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4868 di Mercoledì 10 febbraio 2021

Come raggiungere l'araba fenice: il software sicuro!

Da decenni ormai gli utilizzatori di software cercano di trovare strumenti che garantiscano che l'applicazione che utilizzano sia sufficientemente sicura. Anche l'Europa si sta muovendo in questa direzione.

ENISA-European network security agency, ha pubblicato un documento, che mettiamo in allegato a disposizione dei lettori, che cerca di mettere a punto delle procedure che garantiscano lo sviluppo sicuro di applicazioni software e la loro successiva manutenzione nonché, più in generale, di apparati ICT.

Oggi queste applicazioni sono entrate nella nostra vita quotidiana e un loro funzionamento errato o soggetto ad attacchi dall'esterno può avere conseguenze gravissime sulla società in genere e su specifiche attività.

Il problema non riguarda solo le cosiddette *data breach*, che riempiono le pagine dei giornali tutti i giorni, ma anche anomalie funzionali, che possono portare a gravi conseguenze sulla operatività delle aziende.

Il motivo per cui queste situazioni deplorevoli si verificano è certamente da imputare alla mancata adesione a tecniche e principi fondamentali di sicurezza, in fase di progetto manutenzione.

La adesione a questi principi e tecniche può essere convalidata da processi di certificazione di prodotti e servizi ICT.

Ecco perché ENISA ha deciso di sviluppare un documento preparatorio allo sviluppo di politiche di certificazione dei prodotti, dei servizi e processi, che possano dare una sufficiente garanzia agli utenti circa la affidabilità, resilienza e qualità degli applicativi, che vanno ad utilizzare.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0628] ?#>

Il documento prende in esame vari aspetti, legati allo sviluppo di un progetto di certificazione per il software. Ecco i **principali temi presi considerazione**:

- gli sviluppatori ed i fornitori di prodotti certificati ITC dovrebbero prestare la propria attenzione non solo alla correzione di vulnerabilità, che hanno già assunto una rilevanza diffusa, ma anche per aspetti di sicurezza, in fase di sviluppo, che prendano in considerazione i più comuni rischi afferenti alla sicurezza e li mettano sotto controllo;
- La European Standard Organization e la Standard Developing Organization stanno coordinando le loro attività, in modo da poter mettere a disposizione di venditori ed acquirenti dei processi di standardizzazione, che possano offrire un riferimento oggettivo sul livello di sicurezza degli applicativi;
- gli schemi di certificazione della sicurezza informatica devono includere, per quanto possibile, delle garanzie afferenti non solo alle prestazioni finali del prodotto, ma anche alla conformità alle linee guida, in fase di sviluppo del software, della sua manutenzione del suo utilizzo;
- durante la fase di sviluppo di uno schema di certificazione della sicurezza informatica, valido a livello unione europea, devono essere utilizzati dei metodi più oggettivi di valutazione della conformità, in alternativa agli esistenti strumenti di

validazione, tanto frammentati quanto intrinsecamente carenti;
- infine, gli sviluppatori del software e i produttori di apparati ICT devono mettere a disposizione la loro esperienza e devono impegnarsi a promuovere l'utilizzo di schemi di certificazione informatica, sviluppati a livello europeo.

Il documento allegato analizza in dettaglio questi aspetti e rappresenta un prezioso strumento di riferimento per tutti gli sviluppatori e produttori di applicativi ed apparati ICT.

Adalberto Biasiotti

Enisa, " Advancing software security in the EU. The role of the EU cybersecurity certification framework" (formato PDF, 622 kB)

 Questo articolo è pubblicato sotto una Licenza Creative Commons.
