

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5242 di Lunedì 26 settembre 2022

La sicurezza informatica diventa un problema di dimensioni mondiali

I lettori sono certamente già al corrente della recente istituzione e della piena operatività dell'autorità per la cybersicurezza nazionale, in Italia. Ecco qual è la situazione dall'altra parte dell'Atlantico.

I recenti attacchi portati contro i sistemi informativi dell'Albania, che si ritiene siano stati lanciati dall'Iran, mettono ancora una volta in evidenza come il problema della sicurezza dei sistemi informativi stia acquisendo una dimensione mondiale.

L'Italia ha tempestivamente reagito, istituendo la ACN, Autorità nazionale per la cybersicurezza, che assicura il coordinamento tra i soggetti pubblici coinvolti nella materia. Essa promuove la realizzazione di azioni comuni, volte a garantire la sicurezza e la resilienza cibernetica, necessarie allo sviluppo digitale del Paese.

<https://www.acn.gov.it>

Anche gli Stati Uniti si sono attivati, facendo approvare nel gennaio 2021 una legge sulla difesa nazionale, che ha stabilito l'ufficio del National Cyber Director, che occupa un posto di prestigio nello ufficio esecutivo del presidente degli Stati Uniti.

Pubblicità

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

Allo stesso tempo, questo soggetto costituisce il principale riferimento, per il presidente degli Stati Uniti, per mettere a punto politiche e strategie di sicurezza informatica.

Il compito affidato a questo direttore è oltremodo importante, soprattutto perché a questo soggetto è stato affidato l'incarico di coordinare le strategie di sicurezza informatica delle varie agenzie nazionali degli Stati Uniti, riferendo, una volta all'anno, al Congresso su temi afferenti alle minacce informatiche ea ai problemi specifici che gli Stati Uniti devono fronteggiare.

In particolare, questo soggetto dovrà spingere per garantire un'applicazione uniforme, in tutte le agenzie federali, di norme afferenti alla sicurezza informatica, con particolare riferimento alle infrastrutture digitali degli Stati Uniti.

Questo soggetto dovrà anche migliorare la collaborazione tra pubblica e privato e deve garantire un livello elevato di resilienza, presente e futura, in modo che tutti i responsabili dei sistemi informativi e delle infrastrutture critiche siano pronti a fronteggiare i problemi di oggi e domani.

È interessante rilevare anche il numero di dipendenti che è stato assegnato a questo ufficio: ad agosto 2022 vi sono 55 impiegati, che potranno però salire fino a 75 alla fine di questo anno fiscale.

A questo proposito, può essere interessante confrontare il numero di queste risorse con quelle assegnate alla autorità nazionale per la cybersicurezza, che ad oggi è fissato in 300 esperti, con una dotazione iniziale di 530 milioni di euro, fino a 2027.

È bene far presente ai lettori che non è possibile fare un confronto diretto tra i numeri di queste risorse, in quanto i compiti affidati sono alquanto diversi.

Ad esempio, la nostra Autorità deve anche occuparsi di attivare procedure di valutazione e certificazione nazionale, lavorando anche in stretta collaborazione con il Computer Security Incident Response Team (Csirt) italiano.

Un aspetto significativo, afferente alla operatività dell'ente di cybersicurezza degli Stati Uniti, riguarda la urgenza, che è stata sottolineata, nell'attivazione delle misure di protezione del cyberspazio.

La crescente frequenza e intensità degli attacchi informatici non fanno che confermare come la strategia adottata dall'Italia, dagli Stati Uniti e da molte altre nazioni, sia articolata, sia appropriata e, soprattutto, sia urgente!

Adalberto Biasiotti



Licenza Creative Commons

www.puntosicuro.it