



Cybersecurity: come rendere l'Unione europea più sicura e pronta ad affrontare attacchi informatici

CRONACA, ENINDUSTRY - GRETA BITANTE

11 aprile 2018

Presentato a Bruxelles uno studio di **I-Com. La Commissione Ue lancia un piano strategico contro le minacce online. L'Italia è al dodicesimo posto tra i Paesi più colpiti da attacchi cyber**

Bruxelles – Con le nuove sfide della tecnologia digitale e il boom di internet, l'Unione europea ha bisogno di più sicurezza online. “C'è bisogno di misure per ridurre le minacce degli attacchi online” secondo il presidente dell'**Istituto della competitività (I-com) Stefano da Empoli**. Con la collaborazione dell'Istituto, la Commissione europea ha lanciato un “Piano strategico per la cybersecurity” con lo scopo di aumentare il livello di difesa online e la resilienza dei sistemi di informazione in rete, che è stato presentato oggi al Parlamento europeo a Bruxelles. “E' necessaria un'Unione più sicura per i propri cittadini che navigano online”, spiega il presidente.

Il piano si basa su tre pilastri fondamentali: creare un sistema di difesa europeo forte e resistente per rafforzare la sicurezza in rete in tutti i Paesi membri dell'Ue; reagire concretamente contro i crimini

informatici, adottando misure per penalizzare tali azioni criminali e incoraggiare la cooperazione internazionale per raggiungere gli obiettivi. Uno degli aspetti più importanti della proposta del piano strategico è, secondo **da Empoli**, la creazione di un'Agenzia europea per la cybersecurity che consiste in un rafforzamento delle già esistenti Agenzia dell'Unione europea per la rete e la società informatica (ENISA). Questa misura che avrà effetto permanente sarà resa effettiva nel 2020, alla fine del mandato dell'attuale agenzia. L'**I-Com** sottolinea anche l'importanza di incrementare l'istruzione informatica per avere una maggiore sicurezza online: "Dobbiamo educare le persone perché gli obiettivi del piano vengano raggiunti a livello europeo", afferma **da Empoli**. L'Agenzia europea sulla cybersecurity si concentrerà sulla coordinazione tra gli Stati membri e le istituzioni europee e sulla preparazione e prevenzione di potenziali attacchi informatici. Ciò anche grazie alla creazione di una piattaforma per la formazione a tale scopo creata entro il 2018.

Questi provvedimenti sono stati presi in considerazione dall'**I-Com** e dalle istituzioni europee dopo che il rischio di attacchi in rete è aumentato considerevolmente nel 2017, secondo il WEO sondaggio sulla percezione dei rischi online su scala globale (global risks perception survey). Secondo i dati Eurostat nei Paesi dell'Unione europea il 15% degli utenti internet ha avuto problemi legati alla sicurezza online, come virus, abusi su dati personali e perdite in termini economici. I cittadini che hanno fatto esperienza di attacchi in rete sono stati quelli residenti in Francia (33%), Malta (34%) e Portogallo (36%). L'Italia è al dodicesimo posto per la violazione della sicurezza online (28%).

In particolare, aziende pubbliche e private che operano nel campo dell'energia, dei trasporti, delle banche e nelle infrastrutture digitali devono adottare effettive misure di sicurezza in rete per prevenire rischi e garantire la sicurezza dei sistemi informatici e della rete.