Edge Computing, 5G e aspetti di vulnerabilità delle nuove architetture di rete

Author : Redazione

Date : 14 Maggio 2020

La tanto attesa **"rivoluzione 5G"** è già realtà. Mentre fioriscono ipotesi e interpretazioni circa la portata di tale dirompente innovazione tecnologica, è importante non dimenticare gli aspetti relativi alla sicurezza informatica dei nuovi servizi software e di rete; aspetti complessi e problematici che impongono - sin dalla fase di progettazione - un'attenzione particolare per consentire di contemperare le novità sul piano tecnico con i fondamentali principi di *privacy* e di *security by design*.

Focus di numerosi interventi nell'ambito dei nostri **eventi annuali** Cyber Crime Conference e Forum ICT Security, nonché della scorsa edizione del *bookazine* cartaceo *ICT Security Collection*, il tema è anche stato oggetto di contributi editoriali che ne hanno approfondito caratteristiche tecniche, limiti e potenzialità.

Tra i nostri Autori, in particolare, se ne è occupato diffusamente **Andrea Boggio** con gli articoli *Iper-connessi in sicurezza: la sfida del 5G*, *Edge Computing tra innovazione e sicurezza*, *Divenire-software delle reti e Cyber Security*, nei quali ha evidenziato la centralità delle telecomunicazioni (“infrastruttura essenziale delle comunicazioni digitali”) nel contesto tecnologico contemporaneo e la conseguente necessità di potenziare le misure di sicurezza, a partire da un *Secure Software Developement Life Cycle* sempre più accurato e onnicomprensivo.

Anche **Daniele Rigitano** - dapprima con il contributo *Reti 4G/5G: profili di vulnerabilità e possibili contromisure* e poi nel suo intervento alla Cyber Crime Conference 2019 - ha lavorato sul tema delle reti 4 e 5G, sotto lo specifico profilo delle vulnerabilità (note e ignote) e delle potenziali strategie difensive; come pure **Antonio Manzalini**, che nell'articolo *La sicurezza nell’era del 5G, Edge e Fog Computing* ha messo in luce come “la sempre maggior penetrazione delle connessioni a banda ultra-larga e il dispiegamento pervasivo di risorse IT (Information Technology) più vicine agli utilizzatori” rappresentino “fattori che aumentano i potenziali punti di vulnerabilità e attacco informatico" sottolineando la conseguente, crescente centralità di “soluzioni basate su metodi di *big data analitycs* e Intelligenza Artificiale”.

Infine il gruppo di lavoro formato da **Raffaele Bolla, Maurizio Giribaldi, Giuseppe**

Piro e **Matteo Repetto** ha condiviso con i nostri lettori i risultati di una lunga attività di ricerca scientifica sul tema - sintetizzata nel loro *La sicurezza informatica dei nuovi servizi digitali: un nuovo approccio architetturale* - ribadendo l'esigenza di progettare e sviluppare "nuove soluzioni di cyber security che siano adeguate ai mutati contesti tecnologici e applicativi", al fine di tenere il passo della sempre più "stretta integrazione tra le più recenti tecnologie software (*cloud/edge/fog computing*) e di rete (5G, *Software-Defined Networking*, *Network Function Virtualization* e *Internet of Things*)".

Continueremo, ospitando il punto di vista dei più autorevoli professionisti del settore, a seguire il tema e i relativi sviluppi certi della sua centralità nel panorama presente e futuro della cybersecurity globale.

A cura della Redazione