5G e sicurezza informatica: Synopsys risponde alle esigenze delle TELCO

La riduzione del rischio cyber è ormai un imperativo nazionale poiché le sfide informatiche determinate dall'espansione e compenetrazione di internet in tutte le realtà economiche e sociali rendono indispensabile la messa in sicurezza del cyber spazio.

Il 5G rappresenta certamente la giusta risposta al massiccio aumento delle connessioni, ma apre anche a nuovi scenari di rischio informatico rendendo il bilanciamento di sicurezza, privacy e innovazione imprescindibile nel mondo delle telecomunicazioni.

La "quinta generazione" delle reti mobili, da diversi anni è al centro di suggestioni e remore di ogni tipo. Certamente questa tecnologia, o meglio insieme di tecnologie – definite dall'autorevole US Federal Communications Commission "il prossimo gradiente evolutivo della comunicazione wireless a banda larga" – contribuirà alla diffusione di **ecosistemi digitali sempre più complessi**, dove vedremo sorgere nuove responsabilità a carico degli *Internet Service Providers* (ISP).

Novità legate al 5G: Internet of Things (IoT) ed Edge Computing

Abilitando trasferimenti di dati molto più rapidi e una crescente integrazione tra diversi strumenti il 5G estenderà di fatto la superficie d'attacco attualmente nota, con varie conseguenze in termini di **privacy degli utenti** e perfino di **sicurezza nazionale**. Era perciò inevitabile che si

diffondessero paure – alcune smentite dalla comunità scientifica ma ancora oggetto di studio, come la presunta correlazione con le patologie tumorali – o resistenze – ad esempio sulle possibili interferenze con i sistemi di controllo del traffico aereo – rispetto a una sua prossima adozione, che richiederà comunque tempi e investimenti significativi.

Nelle previsioni degli esperti sarà soprattutto **l'universo IoT** a subire profondi cambiamenti: decuplicando la velocità di upload/download nel trasferimento dati e riducendone drasticamente la latenza, reti e strumenti 5G sapranno portare l'interconnessione tra *devices*, applicazioni e persone a un livello finora difficile da immaginare. Non possono escludersi, ovviamente, effetti rilevanti anche su *cyber-physical systems* e infrastrutture critiche.

La centralizzazione delle risorse avvenuta con il **Cloud Computing** ha portato grandi benefici facendo però emergere problematiche legate alle prestazioni con l'avvento del mobile computing, del modello SaaS e con il proliferare dell'Internet of Things (IoT), innovazioni che hanno palesato la forte necessità di un'architettura distribuita.

In risposta a queste nuove esigenze arrivano 5G e **Edge Computing**, connubio in grado di incrementare contemporaneamente le prestazioni e le funzionalità delle applicazioni.

Il necessario aggiornamento delle prospettive di cybersecurity

Il quadro in cui interverrà tale trasformazione è già piuttosto articolato. Da tempo i Framework del NIST, come di altre importanti organizzazioni, raccomandano **un approccio olistico e proattivo alla gestione del rischio** per consentire alle strategie di sicurezza informatica di evolversi parallelamente alle minacce; nonché di restare aggiornate alle

continue novità tecnologiche e normative, anche sul piano essenziale della *compliance*.

Inserire il 5G all'interno di tale approccio significa dire addio alle applicazioni sinora utilizzate per testare e monitorare gli ambienti operativi. Gli strumenti tradizionali, pensati per rilevare e identificare vulnerabilità già note, rischiano infatti di non riuscire ad assorbire l'impatto delle imprevedibili minacce sorte da questi inediti livelli di interconnessione.

Come gestire i nuovi profili di rischio cyber: la soluzione targata Synopsys

Defensics è la risposta ideale alla necessità di gestire un cambiamento tanto dirompente senza rinunciare alla sicurezza, assumendola invece come fattore abilitante delle tecnologie impiegate.

Tramite tecniche di ***protocol fuzzing*** che supportano oltre 250 diverse tipologie di applicazioni, Defensics consente a ogni azienda di "mettere alla prova" sistemi e protocolli impiegati nelle proprie attività in modo da poterli prontamente aggiornare per prevenire attacchi (anche di tipo *Zero-Day*) o interruzioni di servizio; includendo un'ampia serie di *testing suites* predefinite, oltre a un *software development kit* agile ed efficace, a garanzia della massima adattabilità e semplicità d'uso.

Oggi più che mai è fondamentale affidarsi a partner preparati per tutelare risorse e reputazione aziendali, mantenendo inalterato il proprio vantaggio competitivo. Moltissimi clienti di Synopsys – fra cui spiccano importanti società del mondo TELCO – hanno già scelto Defensics per proteggere i propri *asset* in questa **fase cruciale**, caratterizzata da una profonda innovazione ma anche dall'incertezza che ne deriva, assumendo la giusta postura per affrontare le sfide del 5G alla cybersecurity.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/5g-e-sicurezza-informatica-synopsys-risponde-alle-esigenze-delle-telco/