Computing Continuum e Sicurezza Avanzata nelle Infrastrutture Distribuite

Nel suo intervento al 22° Forum ICT Security, Luigi Romano – professore di Ingegneria Informatica presso l'Università Parthenope di Napoli e presidente del Centro regionale di competenza sull'ICT della Regione Campania – ha approfondito il tema *"Verso un Computing Continuum (IoT, Edge, Cloud e Dataspaces) sicuro"*, fornendo un'analisi dettagliata dell'evoluzione degli scenari di calcolo negli ultimi anni e – verosimilmente – in quelli a venire.

Il concetto centrale è il *"computing continuum"*, che rappresenta una significativa evoluzione nella distribuzione delle risorse computazionali: il relatore ha esposto le relative tecnologie abilitanti, esaminato le principali minacce che interessano tale contesto e analizzato la superficie di attacco che lo caratterizza, delineando strategie sostenibili per garantire la sicurezza in ambienti così complessi.

Successivamente, ha presentato un caso di studio reale in cui queste tecnologie sono già state implementate con successo.

Architettura del Computing Continuum

Il *computing continuum* si basa su un'architettura che realizza un ecosistema in cui la produzione e l'elaborazione dei dati avvengono senza soluzione di continuità, superando i tradizionali perimetri fisici che separavano le diverse aree computazionali. In questo *continuum*, muovendosi da una zona all'altra, si osservano variazioni nei costi delle risorse

computazionali, nella latenza, nella pervasività, nella dipendenza energetica e nella reattività del sistema. Il *cloud* costituisce il nucleo centrale del sistema: la terminologia *"near edge"* e *"far edge"* si riferisce proprio alla distanza rispetto al *cloud*, che rappresenta il cuore dell'infrastruttura computazionale.

Gran parte dell'elaborazione avviene *"on-device"*, quindi su dispositivi indossabili o IoT, situati all'estremità del sistema computazionale.

L'elaborazione *"on-premise"* viene condotta a livello domestico o aziendale.

Nel livello *"far edge"* i dati iniziano ad aggregarsi ed in quello *"near edge"* sono presenti risorse di calcolo collettive su scala nazionale.

Data Space e Sovranità Digitale

il prof. Romano ha ricordato come un elemento fondamentale del *computing continuum* sia l'integrazione dei *data space*, un concetto avanzato che trascende i limiti dei classici *database*, permettendo la condivisione delle informazioni senza necessariamente condividere i dati o comunque garantendo la sovranità sugli stessi.

Un'iniziativa di particolare rilevanza in questo contesto è Gaia-X, che si focalizza sullo sviluppo dei *data space* al fine di promuovere la sovranità digitale europea.

Fiducia e Sicurezza nel Computing Continuum

Una delle caratteristiche chiave del *computing continuum* è il disaccoppiamento tra il livello di fiducia (*trust*) richiesto al sistema e la sua collocazione fisica.

L’esempio condiviso dal relatore ha riguardato un’ipotetica azienda *“Custom Make”* operante nel settore del *Flexible Manufacturing.*



Slide dell’intervento “Verso un Computing Continuum (IoT, Edge, Cloud e Dataspaces) sicuro” tenuto al 22° Forum ICT Security dal prof. Luigi Romano

Tale azienda potrebbe avere diverse sedi fisiche, nonché dei dipendenti in *smart working* o in trasferta, ai quali occorre garantire – nell’interesse dell’azienda – lo stesso livello di fiducia, indipendentemente dalla loro posizione fisica e dal tipo di dispositivo utilizzato per il collegamento. L’obiettivo è, pertanto, garantire un elevato livello di fiducia su tutta l’area logica – non più perimetro – che riguarda l’azienda, senza vincolarlo alla né alla localizzazione geografica né alle risorse computazionali disponibili in loco.

Quando *“Custom Make”* collabora con terze parti, diventa necessario stabilire un livello di fiducia (medio) anche con questi partner. Questo approccio si estende anche ai clienti di prima linea e ad altri partner commerciali, mentre per i partner esterni può essere ridotto.

Anche per i partner e per il mondo esterno, il livello di fiducia non potrà più basarsi sul concetto di *location* tradizionale, né potrà essere influenzato da vincoli computazionali legati alla locazione.

Tecnologie Abilitanti del Computing Continuum

Rispetto alle tecnologie che abilitano il *computing continuum*, nell’intervento sono stati citati il *cloud computing*, l’*Internet of Things* (IoT) e i *data space*.

Il *cloud computing* rappresenta una vera rivoluzione tecnologica, trasformando la capacità di calcolo in una *facility*: vale a dire una risorsa accessibile attraverso qualsiasi rete di connettività, un po' come avviene per l'acqua o per l'energia elettrica.

L'IoT è costituito da dispositivi in grado di raccogliere, elaborare e trasmettere dati; mentre i *data space*, anche alla luce della Strategia Europea per i Dati, offrono nuove opportunità economiche rispetto alla gestione e all'utilizzo delle informazioni.

Superficie di Attacco e Rischi

Nell'ambito del *computing continuum*, la superficie di attacco (*attack surface*) è estremamente ampia e presenta una vasta gamma di rischi, che interessano tanto i dispositivi IoT quanto le risorse *cloud*.

Al riguardo esistono rischi ormai noti al grande pubblico, come gli attacchi contro dispositivi medici o domestici; meno conosciuta è la possibilità di attacchi più sofisticati perpetrati da utenti privilegiati, come amministratori di sistema o *cloud provider*, i quali non necessitano di una fase di *"privilege escalation"*.

Slide dell'intervento "Verso un Computing Continuum (IoT, Edge, Cloud e Dataspaces) sicuro" tenuto al 22° Forum ICT Security dal prof. Luigi Romano

Questi utenti – che includono sia operatori umani sia componenti software, come sistemi operativi e *hypervisor* – rappresentano una delle maggiori sfide di sicurezza, specialmente negli ambienti *cloud*: se non adeguatamente gestiti, i relativi rischi potrebbero causare non solo seri danni agli utenti ma addirittura un crollo del mercato.

Approccio alla Sicurezza: Trusted Computing

Per affrontare le sfide del *computing continuum*, l'approccio proposto dal prof. Romano consiste nell'accettare e gestire le sue complessità intrinseche, come l'eterogeneità dei dispositivi e la limitata sovranità sulle tecnologie che compongono i prodotti ICT.

Nell'impossibilità di ottenere una soluzione ottimale si ricerca quindi una soluzione sub-ottimale ma praticabile, applicando con un approccio di tipo "best effort" il concetto e le funzioni del *"Trusted Computing"* anche a dispositivi non progettati in base a tale paradigma.



Slide dell'intervento "Verso un Computing Continuum (IoT, Edge, Cloud e Dataspaces) sicuro" tenuto al 22° Forum ICT Security dal prof. Luigi Romano

In questo approccio, i vari dispositivi vengono classificati in base al livello di supporto hardware "nativo" per l'implementazione di funzioni di sicurezza: ad esempio valutando se includano un *"Trusted Execution Environment"* (TEE) o un *"Trusted Platform Module"* (TPM), o ancora se non presentino alcuna protezione specifica, per poi sviluppare le soluzioni di sicurezza più adeguate.

Caso di Studio: le Smart Grid

Questa strategia è stata applicata a un caso di studio sulle *smart grid*, un classico esempio di *computing continuum*, sviluppato nell'ambito del progetto europeo CyberSEAS.

L'architettura delle *smart grid*, infatti, racchiude parti *"on-device"* e *"on-premises"* per la generazione e il consumo di energia; una parte *"far edge"* con i concentratori; una parte *"near edge"* per la gestione dei distributori e, infine, il

cloud.

Ciascuna di queste componenti presenta esigenze di sicurezza diverse ma tutte sono interconnesse tra loro, così evidenziando sfide di protezione particolarmente complesse.

Conclusioni

Come evidenziato dall'intervento, il *computing continuum* rappresenta una trasformazione radicale nella gestione delle risorse computazionali: l'integrazione di *data space*, IoT, *edge computing* e *cloud* offre nuove opportunità ma anche significative sfide di sicurezza, richiedendo soluzioni innovative per garantire elevati livelli di fiducia in ambienti altamente eterogenei.

In tale contesto la strategia proposta da Romano suggerisce un percorso verso una sicurezza sostenibile, che tenga conto della natura distribuita e complessa delle moderne infrastrutture computazionali.

Profilo Autore

Luigi Romano è un esperto di sicurezza e affidabilità dei sistemi distribuiti. È Professore Ordinario di Ingegneria Informatica all' Università degli Studi di Napoli "Parthenope", dove ricopre anche il ruolo di Prorettore alle Tecnologie Informatiche. È Presidente del Centro Regionale Information Communication Technology (CeRICT – http://www.cerict.it/en/), il centro di competenza della regione Campania sull'IT. È uno dei cinque fondatori di Trust Up srl (https://www.trustup.it/en/), uno spin-off dell'Università degli Studi di Napoli "Parthenope", specializzato in tecnologie TEE (Trusted Execution Environment). Collabora frequentemente con ENISA, l'Agenzia Europea per la Sicurezza Informatica. È uno degli esperti selezionati da EU-CIP (https://www.eucip.eu/) per la definizione di strategie per la protezione delle

Infrastrutture Critiche. È il Technical Coordinator del progetto CyberSEAS, che ha prodotto importanti risultati sulla cybersecurity dei dataspace.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/computing-continuum/