

Cloud computing forensics: peculiarità e indicazioni metodologiche – Vincenzo Calabrò



Alla Cyber Crime Conference 2024, Vincenzo Calabrò, Funzionario alla Sicurezza CIS (Ministero dell'Interno) e Digital Forensics Analyst, ha tenuto una presentazione illuminante su un tema d'attualità nel campo della sicurezza informatica: la "Cloud Computing Forensics". Questo argomento, essenziale per la comprensione delle dinamiche moderne di sicurezza e investigazione digitale, riguarda principalmente i contenziosi che emergono con l'uso estensivo del Cloud nelle organizzazioni, sia pubbliche che private.

Guarda il video completo dell'intervento:

[embedded content]

Aree di Contenzioso nel Cloud Computing

Calabrò ha identificato tre aree principali di contenzioso in ambito Cloud Computing:

- questioni contrattuali e civilistiche relative agli accordi di livello di servizio (SLA);
- violazioni della sicurezza dati, che includono integrità, confidenzialità e disponibilità;
- uso improprio del cloud per commettere ulteriori reati, come il mining illegale di criptovalute o la diffusione di materiale illegale.

Queste aree riflettono i cambiamenti dei paradigmi di sicurezza informatica e le sfide poste dalla transizione verso

la “nuvola”.

Modelli di Deployment del Cloud e Sfide per la Sicurezza

Un focus particolare della sua discussione è stato il modello di Deployment del Cloud, che può essere pubblico, privato, ibrido o multi-cloud. Calabrò ha sottolineato come il passaggio dai sistemi on-premise ai modelli basati su cloud comporti una trasformazione nel controllo e nella responsabilità, oltre a una diversa gestione della sicurezza, ponendo nuove sfide per gli investigatori digitali.

Investigazioni Digitali, la Responsabilità dei Provider di Servizi Cloud

Nell'investigazione forense del Cloud, la responsabilità si sposta significativamente verso i provider di servizi Cloud. Questo cambio di paradigma richiede una comprensione approfondita delle configurazioni e dei servizi offerti dai provider per poter identificare e isolare i dati rilevanti in caso di indagine. Calabrò ha evidenziato l'importanza di comprendere l'elasticità, la scalabilità e la flessibilità del Cloud, caratteristiche che, se da un lato offrono vantaggi in termini di efficienza e costi, dall'altro lato introducono complessità nelle indagini forensi, come la difficoltà nel determinare la precisa locazione fisica dei dati.

Strategie per Superare le Sfide della Cloud Forensics

La presentazione ha anche delineato le strategie per superare le sfide poste dalla Cloud Forensics, raccontando la necessità di acquisire una conoscenza dettagliata delle specifiche tecniche del Cloud, come i Log di sistema e i meccanismi di

Detection e Response perché possono rappresentare una notevole fonte di prova. Ha messo in luce l'importanza di collaborare con i provider di servizi Cloud durante le indagini e di utilizzare strumenti forensi avanzati per acquisire dati in modo sicuro e conforme alle normative vigenti.

“Acquisizione Virtuale” e Giurisdizione nel Cloud

Inoltre, ha esplorato il tema di “acquisizione virtuale”, che differisce significativamente dalle tecniche tradizionali di sequestro fisico usate nei sistemi on-premise. Questo processo implica la creazione di copie digitali di dati, macchine virtuali o container, che devono essere gestite con estrema cautela per preservarne l'integrità e garantire che l'analisi sia replicabile e verificabile.

Un punto saliente della discussione è stata l'attenzione alla giurisdizione e alla multitenancy nel Cloud, che possono complicare ulteriormente le indagini a causa della distribuzione geografica dei dati e della condivisione di risorse tra diversi clienti.

Proattività nella Definizione dei Contratti con i Provider

Calabrò ha proseguito suggerendo l'adozione di una strategia proattiva nella definizione dei contratti con i provider, insistendo sulla necessità di clausole chiare che indichino la gestione dei dati e le responsabilità in caso di incidenti.

Competenze Digitali e Formazione in Ambito Cloud

Concludendo, il relatore ha sottolineato la crescente importanza delle competenze digitali e forensi in ambito Cloud per gli operatori della sicurezza. Ha raccomandato un continuo

aggiornamento professionale e un maggiore focus sulla formazione specifica per il Cloud, al fine di preparare adeguatamente i professionisti della sicurezza a fronteggiare le sfide emergenti nel panorama della cyber security moderna.

Il programma completo della Cyber Crime Conference 2024 è disponibile al seguente link:
<https://www.ictsecuritymagazine.com/eventi/cybercrimeconference2024#programma>

Iscriviti alla nostra newsletter per rimanere aggiornate sulle nostre iniziative:
<https://www.ictsecuritymagazine.com/newsletter/>

Condividi sui Social Network:
<https://www.ictsecuritymagazine.com/cybersecurity-video/cloud-computing-forensics-peculiarita-e-indicazioni-metodologiche-vincenzo-calabro/>