SERVIZI UCC IN CLOUD E SICUREZZA: QUALE APPROCCIO?

Paolo Manzoni

Nicola Sfondrini

L'esigenza di comunicare è antica quanto l'uomo ma "l'essere connessi" è ormai diventata una necessità basilare per svolgere la quasi totalità delle nostre azioni quotidiane.
Per le aziende questo concetto è estremizzato, sia quando si parli di una "connessione" interna alla azienda (tra colleghi), sia quando la relazione di contatto si indirizza a soggetti terzi esterni all'azienda, clienti o fornitori.
Per questo, le funzionalità che sono identificate dal termine Unified Collaboration and Communication (UCC), sono considerate sempre più come un bisogno imprescindibile per garantire l'agilità e la flessibilità richiesta nel mercato dei nostri giorni, iper competitivo, digitale e in continua trasformazione.
Da una analisi condotta da IDC sui servizi UCC si evince che il 61 % delle aziende, nei prossimi tre anni, ha pianificato l'adozione di questi servizi sia in termini di ampliamento che prima adozione determinando una stima di crescita del 9% già nel 2016 del budget medio destinato a questi servizi UCC.
Ma è l'avvento e il consolidamento del paradigma Cloud che ha portato alla disponibilità sul mercato di soluzioni "**Unified Communications and Collaboration as a Service**" (UCCaas) adatte a qualsiasi piattaforma e qualsiasi tipo di dispositivo, abilitando nuove modalità di lavoro anche in mobilità e nuovi processi di relazione più veloci ed efficaci (si pensi alle chat, alle videoconferenze, ecc.) con i quali anche il consumer si trova a proprio agio.
La possibilità di interagire in tempo reale con diversi attori e la facilità nello scambio di informazioni e documenti rendono questi sistemi estremamente attrattivi. Tuttavia, se da un lato favoriscono l'incremento della produttività aziendale e il miglioramento della ***customer satisfaction***, dall'altro incontrano resistenza all'adozione suscitando preoccupazione per i potenziali rischi, legati alla difficoltà di controllo nel caso in cui non vengano adottate opportune policy nella gestione del servizio e prassi corrette nelle modalità di utilizzo.
Sicurezza e privacy sono le due parole che in questo caso sintetizzano i problemi e i rischi potenziali associati ad un errato o non governato utilizzo di servizi UCCaas. Infatti, malgrado il Cloud sia ormai un trend tecnologico consolidato, la percezione di perdita di controllo sui sistemi e di possibili attacchi da parte di cyber criminali è ancora molto diffusa in diversi contesti aziendali non sempre preparati ad affrontare queste tematiche con i mezzi e le competenze necessarie.
Spesso viene commesso l'errore di considerare il tema sicurezza un puro e unico aspetto tecnico, senza considerare l'aspetto umano e comportamentale che coinvolge ed interessa tutte le funzioni aziendali e tutte le risorse.
L'azienda che adotta servizi UCCaas deve prepararsi all'utilizzo corretto degli strumenti e seguire approcci metodologici sia nella valutazione delle caratteristiche tecniche di gestione della sicurezza del servizio offerto, sia nelle modalità di utilizzo da parte dei propri utenti, predisponendo opportuni programmi di formazione per garantire il corretto "imprinting".
Questo sforzo, spesso non banale, non può essere improvvisato e deve essere disegnato sulla base delle caratteristiche dell'azienda e della strategia ICT di breve e medio termine con un approccio metodologico e il supporto di buone pratiche (*best practicies*).
Molte infatti sono le domande che nascono quando si affronta un progetto di adozione dei servizi UCC in modalità "as a service".
Forum UCC + Social[1] **e CSA Italy**[2] hanno deciso di avviare uno studio[3] per fornire una visione aggiornata sulla sicurezza dei sistemi UCCaaS in Italia e per suggerire buone pratiche in grado di semplificarne e migliorarne l'adozione. Lo studio vedrà come primo passo il lancio di una *survey* per raccogliere da un campione significativo di aziende (sia lato business che ICT) le priorità da indirizzare per favorire l'utilizzo sicuro di questi servizi.
Nell'analisi preliminare sono state evidenziate **quattro macro-aree** in cui ricadono le principali problematiche che impattano i sistemi UCCaaS e i dati da essi trattati: **Applicazioni, Rete, Sistemi e Legale**.

> **IL CONSOLIDAMENTO DEL PARADIGMA CLOUD HA PORTATO ALLA DISPONIBILITÀ SUL MERCATO DI SOLUZIONI "UNIFIED COMMUNICATIONS AND COLLABORATION AS A SERVICE" (UCCAAS) ADATTE A QUALSIASI PIATTAFORMA E QUALSIASI TIPO DI DISPOSITIVO**

Paolo Manzoni: ingegnere elettronico, classe 1957, ha dedicato il suo impegno lavorativo principalmente alle tematiche ICT prima in IBM e quindi come CIO in grandi gruppi italiani del settore energy & utilities. Ha ricoperto cariche nei board di aziende di scopo dei gruppi per cui ha lavorato ed è stato Presidente di Selene bs. Oltre ad una profonda esperienza di trasformazione e sviluppo delle strutture ICT, delle achitetture HW/SW e dei servizi, ha potuto negli anni sviluppare una conoscenza specifica del settore energy & utilities e degli ambiti di applicazione delle tecnolgie digitali per innovare il business di tali aziende, guidando anche team dedicati a progetti di ricerca e sviluppo nel campo delle smartgrid-smartcity.

Nicola Sfondrini: è laureato con lode in ingegneria informatica presso l'Università degli studi di Pavia ed è attualmente Executive PhD candidate con una tesi di ricerca sul calcolo distributo in ambienti Cloud e Fog Computing. Dal 2011 lavora in Business Integration Partners, dove è oggi Associate Manager e gestisce progetti internazionali in ambito Cloud Computing e data centre optimisation. Socio di CSA Italy e coordinatore dell'area di ricerca "Portabilità, interoperabilità e sicurezza applicativa".

CSA Italy è un'associazione no profit italiana nata nel 2011 come capitolo nazionale dell'associazione internazionale CSA (Cloud Security Alliance) a cui aderiscono le maggiori aziende del settore ICT ed Information Security che hanno scelto il Cloud Computing come parte rilevante del loro business. CSA coordina una community di professionisti che contribuiscono attivamente a sviluppare linee guida e buone pratiche per uno sviluppo ed utilizzo in sicurezza del Cloud.

Il **Forum UCC+Social** si occupa di Unified Communication e Social Collaboration. Promuove la diffusione delle tecnologie e dei servizi UCC e la crescita di conoscenze e professionalità su adozione, affidabilità e performance nella sua comunità.Organizza speciali eventi e premi per aziende e responsabili, realizza webinar ed effettua indagini on-line.

1 www.forum-ucc.it
2 www.cloudsecurityalliance.it
3 I coordinatori dello Studio sono Nicola Sfondrini (CSA Italy) e Paolo Manzoni (Forum UCC+Social)

LA SICUREZZA DEI SISTEMI UCCAAS NON È SOLO UN PURO ASPETTO TECNICO, MA IMPLICA ANCHE L'ASPETTO UMANO E COMPORTAMENTALE CHE COINVOLGE ED INTERESSA TUTTE LE FUNZIONI AZIENDALI E TUTTE LE RISORSE

Dal punto di vista applicativo, il servizio UCCaas erogato dal fornitore deve includere:

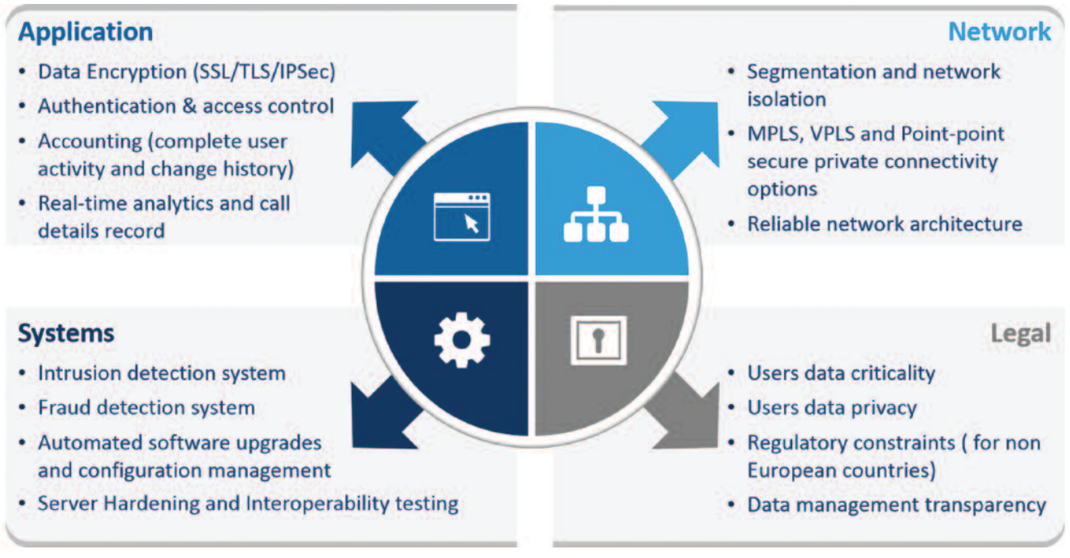
- Caratteristiche di sicurezza quali ad esempio l'encryption dei dati tramite protocolli standard, garantendo così il corretto livello di privacy, senza compromettere le performance;
- Una gestione degli accessi idonea a riconoscere anche eventuali account compromessi, creando una cronologia accurata da utilizzare in caso di identificazione di una intrusione;
- Se i fornitori di servizi devono dotare la propria offerta di tali caratteristiche, spetta alle aziende utilizzatrici assicurarsi della presenza di strumenti di verifica del servizio erogato anche basati sull'utilizzo di soluzioni real-time analytics collegate con i sistemi di *monitoring* e di *ticketing* per facilitare ed automatizzare l'analisi delle funzionalità UCCaaS ed identificare eventuali comportamenti anomali.

Per quanto riguarda **i sistemi e l'infrastruttura hardware e software** sottostante:

- i fornitori di servizi UCCaas devono garantire la riduzione delle potenziali vulnerabilità attraverso uno strutturato approccio di *hardening* supportato da sistemi automatici per l'installazione di update software e di patch di sicurezza, assicurando al contempo la continuità del servizio;
- le aziende utilizzatrici devono valutare in fase di offerta le peculiarità del servizio anche da questo punto di vista e ottenere fin dove possibile l'accesso a strumenti di controllo e verifica della corretta gestione e aggiornamento.

La rete è certamente un altro componente essenziale da proteggere adeguatamente; in questo caso occorre:

- Che i fornitori adottino protocolli standard per evitare lo *sniffing* dei pacchetti durante il transito da un nodo all'altro ed eventuali tecniche di segmentazione per limitare i movimenti nel caso di accessi non autorizzati;
- Che le aziende utilizzatrici indaghino meglio le modalità di accesso e utilizzo della rete adeguando eventualmente anche le proprie componenti interne alle proprie sedi.



LA RICERCA DI CSA ITALY E UCC FORUM + SOCIAL HA EVIDENZIATO QUATTRO MACRO-AREE IN CUI RICADONO LE PRINCIPALI PROBLEMATICHE CHE IMPATTANO I SISTEMI UCCAAS E I DATI DA ESSI TRATTATI: APPLICATIONS, NETWORK, SYSTEMS E LEGAL

Infine risulta altrettanto importante l'analisi degli **aspetti legali** e normativi per non fronteggiare i rischi derivanti dalle differenze legislative vigenti nelle diverse aree geografiche. Ad esempio è importante conoscere con precisione il luogo dell'effettiva archiviazione dei dati e quali persone siano coinvolte per garantire la conformità con le relative leggi, monitorare la situazione richiedendo una approccio trasparente.

Nella survey verranno indirizzati anche gli aspetti "culturali", poichè possono costituire una vulnerabilità nell'impianto di sicurezza complessiva esponendo le aziende a potenziali compromissioni, anche importanti. Infatti, una non adeguata formazione in ambito security degli utenti e una tendenza a mantenere comportamenti "abitudinari" spesso non in linea con le policy di sicurezza prestabilite, possono compromettere la sicurezza e privacy anche nelle migliori implementazioni.

Da una recente analisi condotta da CSA[4] è emerso che in molti casi la nomina di un *executive* al ruolo di Chief Information Security Officer (CISO) contribuisce sia ad influenzare positivamente il *mindset* aziendale sia a stimolare una partecipazione di tutte le risorse e Funzioni aziendali nella corretta gestione della sicurezza e privacy dei dati. ■

LA CREAZIONE DI UNA CULTURA DI SICUREZZA AZIENDALE RAPPRESENTA UN PASSAGGIO FONDAMENTALE PER LA RIDUZIONE DELLE VULNERABILITÀ A CUI I SISTEMI UCCAAS SONO ESPOSTI

4 https://cloudsecurityalliance.org/media/news/csa-survey-64-9-of-it-trusts-the-cloud-as-much-or-more-than-on-premises-solutions/