Comunicazioni e collaborazione sicure in cloud con Avaya Cloud Office

Tra le molte domande che le aziende si pongono quando valutano il passaggio al cloud, la sicurezza spesso si trova al primo posto. In particolare, la natura sensibile delle comunicazioni aziendali, con i dipendenti e i clienti, è un argomento fondamentale per i team addetti alla sicurezza. Dopo tutto, ogni giorno i dipendenti chiamano, inviano messaggi, tengono riunioni, inviano fax, e-mail e utilizzano altre forme di comunicazione per condividere strategie ed informazioni che definiscono il loro vantaggio competitivo.

Nel mondo di oggi, la sicurezza dei dati rappresenta una priorità assoluta per le azienda. In qualità di fornitori di soluzioni UCaaS, comprendiamo le implicazioni per la sicurezza del modello cloud. Per noi la sicurezza è una priorità per proteggere le nostre operazioni e i dati dei clienti. I nostri servizi cloud sono progettati per offrire sicurezza di primo livello ed in quanto cliente di Avaya Cloud Office, potrai usufruire delle best practice integrate nelle nostre policy, nell'architettura e nei processi operativi, messi a punto per rispondere ai requisiti di sicurezza dei clienti. Questo white paper offre una panoramica su sicurezza e affidabilità offerte dai nostri prodotti e servizi.

Team addetto alla sicurezza e sicurezza dell'organizzazione

La sicurezza inizia dalla nostra cultura. La sicurezza e la fiducia dei clienti sono valori aziendali fondamentali, e noi li integriamo nei nostri servizi, investendo in sicurezza dedicata.

Nell'ambito della nostra struttura organizzativa, abbiamo un reparto dedicato alla sicurezza, con ingegneria della sicurezza, verifica/conformità della sicurezza, sicurezza delle applicazioni, analisi dei dati di sicurezza e funzioni di abuso di servizio che fanno riferimento al Responsabile della Sicurezza (CSO) della società.

Inoltre, effettuiamo verifiche sul background dei dipendenti, teniamo corsi di formazione sulle procedure di sicurezza ai nuovi assunti e ai dipendenti, che ogni anno sono tenuti ad accettare le policy aziendali, inclusa la nostra policy sulla sicurezza.

Tutti i dipendenti ricevono una formazione approfondita sulla protezione dei dati e sulla riservatezza, nonché sulla sicurezza delle informazioni. Questo tipo di formazione sulla sicurezza è obbligatorio e ha luogo almeno una volta all'anno.

Tutti i dipendenti ricevono una formazione approfondita sulla protezione dei dati e sulla riservatezza, nonché sulla sicurezza delle informazioni. Questo tipo di formazione sulla sicurezza è obbligatorio e ha luogo almeno una volta all'anno.

Tutti i dipendenti devono accettare e sottoscrivere un accordo di protezione e riservatezza dei dati. Dopo la formazione e la valutazione, tutti i dipendenti ricevono inoltre un certificato di completamento.

Sicurezza di Avaya Cloud Office

Il nostro impegno per la sicurezza non teme paragoni. Il nostro impegno è sostenuto da un team globale di esperti sulla sicurezza informatica che partecipano non solo alla pianificazione e allo sviluppo della piattaforma, ma anche alle operazioni quotidiane.

Noi ci occupiamo di implementare:

- Sviluppo di software sicuri
- Efficaci controlli degli accessi
- Servizi resilienti
- Rilevamento e mitigazione delle minacce
- Controlli delle operazioni di servizio
- Amministrazione clienti e controlli utenti
- Supporto integrato per gli obblighi normativi
- Application programming interfaces (API) sicure
- Integrazioni preconfigurate
- Trasparenza

Il seguente modello di sicurezza cloud illustra l'approccio che adottiamo per realizzare questi obiettivi di sicurezza:

Governance: gestione e misurazioni dei rischi	
Amministrazione dei servizi degli utenti	Controllata dal cliente
Sicurezza delle applicazioni	Progettata e testata internamente
Sicurezza dei confini	Inserimento dei dati in Cloud di Servizio
Sicurezza dei dati	Dati crittografati in transito e a riposo
Sicurezza della piattaforma	Infrastruttura e operazioni
Mitigazione delle frodi telefoniche	Rilevamento e interruzione dell'abuso dei servizi
Sicurezza fisica	Ambienti protetti
Verifica indipendente	Verifiche e test di sicurezza di terze parti

Sicurezza fisica

I nostri servizi sono ospitati globalmente nei data center di tipo enterprise di livello 4 e nei principali cloud pubblici. La sicurezza e la disponibilità sono condizioni essenziali quando selezioniamo le nostre sedi per l'erogazione dei servizi. Questi ambienti garantiscono sicurezza fisica, controlli ambientali e operazioni in sede all'avanguardia. I centri operativi di rete (Network Operations Centers, NOC) sono costantemente monitorati 24 ore su 24, 7 giorni su 7 e gestiti in loco da tecnici specializzati. L'ingresso in ogni data center prevede l'identificazione biometrica, nonché la doppia autenticazione della persona e un sistema integrato di "man trap". I sistemi di sicurezza vengono controllati mensilmente per garantire la massima protezione e ogni data center è conforme allo standard SSAE 18.

Gestione degli accessi

L'accesso agli ambienti di produzione è rigorosamente controllato tramite la Gestione di Identità e Accessi (IAM) e controlli di accesso a più fattori. Queste efficaci misure per la gestione degli accessi consentono l'accesso ai nostri ambienti di produzione solo al personale autorizzato.

Crittografia dei dati

La crittografia dei dati protegge i dati sensibili dei clienti e delle chiamate da accessi non autorizzati. Tutti i dati dei clienti vengono crittografati in transito e a riposo, utilizzando crittografia, standard e protocolli leader del settore.

Noi ci avvaliamo di due protocolli di sicurezza di livello enterprise per garantire ulteriore sicurezza per le chiamate IP - autenticazione TLS e crittografia SRTP:

il Transport Layer Security (TLS) è un protocollo crittografico che garantisce la crittografia dei dati della segnalazione del Session Initiation Protocol (SIP). Questo protocollo protegge la comunicazione della segnalazione SIP tra dispositivi endpoint supportati e i nostri server cloud.

Il Secure Real-Time Transport Protocol (SRTP) è un profilo del Real-Time Transport Protocol (RTP) che offre crittografia, autenticazione e integrità dei messaggi, nonché la protezione anti-replay del flusso di pacchetti RTP che viene trasportato tra dispositivi endpoint supportati e i nostri server cloud.

Inoltre, tutti i portali Internet si avvalgono di protocolli sicuri e crittografati (SSL Certificate / https); tutti i dati non vocali dei clienti sono crittografati TLS; i telefoni VoIP utilizzano certificati digitali per stabilire connessioni sicure per il download dei dati di provisioning.

Sicurezza della rete

Abbiamo implementato le migliori protezioni di rete ottimizzate per voce e dati. Queste protezioni, unitamente al costante monitoraggio dei sistemi da parte dei nostri esperti per escluderne anomalie, contribuiscono a prevenire interruzioni di servizi, violazioni di dati, frodi e hijacking di servizi.

AVAYA

Gestione delle vulnerabilità

Abbiamo implementato pratiche di rafforzamento dei sistemi e automatizzazione della scansione continua delle vulnerabilità delle risorse di produzione. Sottoponiamo a scansione server, dispositivi di rete e altri sistemi per identificare vulnerabilità non corrette e problemi di mancata conformità con le configurazioni di sicurezza previste. Una volta identificata una vulnerabilità che richiede una correzione, questa viene registrata, le viene assegnata una priorità in base alla gravità e un titolare responsabile.

Gestione delle patch

Nell'ambito delle sue iniziative di gestione delle vulnerabilità, Avaya Cloud Office include la gestione delle patch. Alle patch vengono assegnate priorità e la loro installazione avviene in base agli standard interni di definizione delle priorità. Tutte le patch vengono testate su sistemi di non produzione prima dell'installazione sui sistemi di produzione.

Gestione delle modifiche

Disponiamo di un processo di gestione delle modifiche molto accurato. Le pratiche di controllo delle modifiche prevedono riunioni con cadenza regolare per controllare e gestire le modifiche apportate al nostro ambiente di produzione. Prima dell'implementazione nella produzione, le richieste di modifica sono documentate e approvate da più stakeholder. Al momento dell'implementazione, vengono adottate procedure di verifica per garantire che le modifiche vengano apportate con successo. Nel caso in cui le varie fasi di verifica non vadano a buon fine, disponiamo di procedure e policy di ripristino. Implementiamo monitoraggio delle configurazioni, monitoraggio dei flussi, EDR e altre misure di monitoraggio.

Sicurezza delle applicazioni

Implementiamo costantemente best practice per lo sviluppo di software, al fine di garantire la sicurezza durante tutte le fasi di sviluppo, realizzazione, distribuzione e rilascio di qualsiasi progetto software, tra cui:

Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) e Runtime Application Security Testing (RAST)

- Scansione delle applicazioni
- Analisi delle librerie di terze parti
- Impegni firmati
- Analisi della composizione del software
- Scansione delle Application programming interface (API)
- Test di penetrazione

Sviluppo di software sicuri

Durante il processo del ciclo di vita dello sviluppo software, che comprende corsi di formazione su codici sicuri per tutti gli sviluppatori, noi garantiamo la sicurezza e adottiamo best practice.

Nell'ambito del processo di gestione delle vulnerabilità, vengono controllate regolarmente le prime 10 vulnerabilità OWASP e i primi 25 errori di software CWE.

Piattaforma per gli sviluppatori

Gli sviluppatori di un'applicazione su Avaya Cloud Office devono utilizzare la Open Authentication (OAuth), che impedisce la trasmissione delle credenziali del cliente al server dell'applicazione e dello sviluppatore. Dopo aver richiesto l'accesso all'applicazione di terzi, i clienti vengono indirizzati al nostro portale, dove inseriscono il nome utente e la password. Durante questo processo, i clienti vengono informati delle autorizzazioni esatte che l'applicazione richiede e possono annullare la richiesta in qualsiasi momento.

Se un cliente accetta la richiesta di autorizzazioni dell'applicazione, il server dell'applicazione e dello sviluppatore riceve un token portante che può essere utilizzato per operare per conto del cliente. Se non viene aggiornato dall'applicazione, il token scade e può essere revocato da noi o dal cliente in qualsiasi momento tramite il Portale Admin.

Per le applicazioni private destinate all'uso esclusivo da parte dell'organizzazione che le ha create, gli sviluppatori possono utilizzare il proprio nome utente e la propria password per richiedere un token portante. Questo processo consente di oscurare le credenziali del cliente impedendo l'uso e il posizionamento multiplo delle sue credenziali. Tuttavia, poiché non esiste alcun modo per impedire l'accesso alle credenziali dei clienti qualora l'applicazione o il server subissero un attacco, questo metodo è sconsigliato.

Ogni sviluppatore esterno sulla piattaforma deve disporre di un account sviluppatore in cui registra e imposta le autorizzazioni per le loro applicazioni. A ogni applicazione viene assegnato un ID cliente e una credenziale segreta del cliente. Ciò consente il monitoraggio di ogni singola applicazione che, se necessario, verrà aggiornata o terminata qualora la sicurezza dell'applicazione risulti compromessa o l'intenzione dell'applicazione diventi dannosa.

Oltre a disporre di un ID cliente univoco e di credenziali segrete, gli sviluppatori devono impostare autorizzazioni specifiche che verranno utilizzate dalla loro applicazione. Se un'applicazione richiede più autorizzazioni del necessario,

non potrà essere utilizzata in produzione fino a quando tali autorizzazioni non saranno utilizzate o rimosse dalla portata dell'applicazione. In questo modo, si evita che le richieste di autorizzazione vengano utilizzate in modo improprio o se ne abusi. Come ulteriore livello di sicurezza delle applicazioni, ogni applicazione deve superare un approfondito processo di valutazione, che comprende una verifica manuale del nome, della descrizione, delle autorizzazioni richieste e dei limiti della velocità dell'applicazione. Sono inoltre previsti controlli automatici per garantire che l'applicazione non abbia errori di chiamata API o tassi di errore elevati, garantendo al contempo che non utilizzi alcuna autorizzazione non richiesta o che non siano state richieste autorizzazioni che non vengono utilizzate. Gli sviluppatori, inoltre, non sono in grado di modificare il loro tipo di applicazione o le autorizzazioni richieste una volta che l'applicazione è stata resa pubblica.

Rilevamento e mitigazione delle minacce

Il nostro servizio consiste di molteplici misure atte a prevenire e rilevare interruzioni dei servizi, acquisizione di account, abuso di servizi e frodi delle telecomunicazioni, tra cui monitoraggio delle operazioni dei servizi, controlli degli accessi, controlli di rilevamento, limitazione dell'uso e piani di composizione internazionale controllati dal cliente. Noi implementiamo le funzionalità del Unified Communications Threat Management (UCTM) per facilitare il rilevamento e la mitigazione delle chiamate robo-call e altre forme di chiamate indesiderate. Inoltre, il nostro reparto di sicurezza esegue il monitoraggio attivo per rilevare e avvisare i clienti di attività di accesso sospette, dispositivi non riconosciuti e modelli di chiamata anomali sul loro account.

Continuità del servizio e ripristino di emergenza

Abbiamo la nostra infrastruttura tecnologica principale e la rete globale in più data center di livello 4 all'avanguardia, distribuiti in diverse aree geografiche, cosa che riduce al minimo il rischio di perdita e interruzione del servizio dovute a disastri naturali e altre catastrofi.

All'interno di ogni data center principale, forniamo un'architettura ridondante di high availability. I nostri componenti di servizio sono progettati tenendo ben presenti un'alto livello di disponibilità, la tolleranza d'errore e l'impatto degli errori. I dati dei clienti, comprese le configurazioni e i messaggi del servizio, sono completamente replicati in tempo reale nei nostri data center.

In caso di guasto, i nostri sistemi automatizzati, in combinazione con un centro operativo di rete (NOC) sempre attivo e di primo livello, garantiscono una rapida transizione ai sistemi di backup, in base alle necessità, per assicurare l'ininterrotta disponibilità del servizio. Inoltre, eseguiamo periodicamente test di ripristino di emergenza per valutare l' alta disponibilità del sistema al fine di assicurare l'esperienza cliente migliore e più semplice possibile.

Modello di separazione logica e multi-tenancy

Noi mettiamo a disposizione dei nostri clienti un ambiente multi-tenant e manteniamo un elevato livello di sicurezza per garantire che i dati di un cliente non siano mai disponibili a un altro cliente. Utilizziamo un'architettura multi-tenant e visualizzazioni dinamiche del database per formare gli strati limite delle applicazioni tra le istanze dei clienti.

AVAYA

Sicurezza dell'account come responsabilità condivisa

Controlli amministrativi del cliente
Avaya Cloud Office, come la maggior parte dei fornitori di soluzioni cloud, opera in base a un modello di responsabilità condivisa per la sicurezza. Tale modello identifica le responsabilità condivise tra il cliente e il fornitore del cloud. Siamo responsabili della fornitura, dell'architettura e della sicurezza del servizio core, nonché della sicurezza fisica e ambientale dell'infrastruttura implementata per prestare il nostro servizio.

I nostri clienti hanno la responsabilità di gestire le politiche inerenti al loro account, concedere agli utenti i ruoli e le autorizzazioni del caso, implementare correttamente il Single Sign-on, tracciare le modifiche amministrative apportate al loro account, controllare i piani di composizione internazionali e collaborare con noi per identificare attività sospette. Tra i controlli amministrativi a disposizione degli amministratori vi sono:

Ruoli e autorizzazioni
I controlli di accesso basati sul ruolo assicurano un ulteriore livello di sicurezza per favorire il rispetto delle politiche sulla sicurezza aziendale, garantendo una supervisione completa sulle autorizzazioni utilizzate. Lo stesso livello di accesso viene concesso unilateralmente a ogni utente assegnato a tale ruolo, al fine di garantire la semplice adozione e preservazione di un approccio coerente. È possibile creare ruoli per funzioni o posizioni nell'azienda con l'integrazione di tutte le autorizzazioni appropriate. Abbiamo messo a punto sette ruoli standard pronti all'uso per accordare rapidamente a molti utenti contemporaneamente il giusto livello di accesso al sistema, eliminando gli errori che possono verificarsi quando le autorizzazioni vengono impostate individualmente. È possibile definire ruoli personalizzati per supportare innumerevoli combinazioni di autorizzazioni, estendendo la gamma di controllo granulare su come gli utenti possono accedere alle funzionalità. Per ogni ruolo è possibile selezionare le autorizzazioni esatte che si desidera concedere e aggiornare le selezioni in qualsiasi momento.

Elenco operazioni
Gli elenchi operazioni consentono ai clienti di tenere traccia delle modifiche della configurazione apportate a un account per scopi di verifica e risoluzione dei problemi. È possibile identificare tentativi di accesso, modifiche a numeri di telefono, acquisti di licenze e altre modifiche alle impostazioni e alle autorizzazioni di amministratore/dipendente.

Sign-On Singolo (SSO)
Offriamo funzionalità SSO che rendono i login senza interruzioni a tutti i livelli. Anche se il sistema SSO è pratico per gli utenti, presenta anche nuove sfide per la sicurezza. Se la password principale di un utente risulta compromessa, i pirati informatici possono essere in grado di accedere a più risorse. Inoltre, dato che le informazioni sensibili arrivano ai servizi basati sul cloud, è ancora più importante proteggere l'accesso implementando l'autenticazione a due fattori.

Gli amministratori possono definire politiche che prevedono controlli specifici per ogni singola applicazione SSO, cosa che implicherebbe un doppio controllo dell'utente, del dispositivo e della rete rispetto alla politica relativa a un'applicazione prima di consentire l'accesso alla stessa. Ad esempio, gli amministratori potrebbero richiedere che gli utenti CRM completino l'autenticazione a due fattori ad ogni accesso, ma solo una volta ogni sette giorni quando accedono alla soluzione core.

Verifica indipendente

Oltre alle misure di sicurezza implementate nell'ambito dell'infrastruttura fisica e cloud, veniamo sottoposti a verifiche indipendenti e audit dei nostri controlli di sicurezza da parte dei principali partner e terzi. Queste valutazioni garantiscono il soddisfacimento delle esigenze di conformità dei nostri clienti. Ci adoperiamo particolarmente per rispettare le normative poste da settori specifici.

Oltre alle misure di sicurezza adottate a livello di tutto lo sviluppo dei prodotti, gli ambienti di produzione e le operazioni di servizio, incarichiamo anche revisori esterni di esaminare i nostri controlli di sicurezza. Queste valutazioni garantiscono che le nostre protezioni siano sottoposte a verifiche e test, e rese visibili ai nostri clienti. Ci adoperiamo particolarmente per rispettare le normative poste da settori specifici e le leggi in materia di privacy di dati. Alcuni esempi:

Certificazioni e rapporti

SOC 2 Tipo II
Il rapporto SOC 2 conferma l'efficacia dei nostri controlli operativi quale organizzazione di servizi in base ai criteri stabiliti dai Principi dei servizi fiduciari dell'**American Institute of Certified Public Accountants (AICPA)**. Ogni anno veniamo sottoposti a una verifica di terze parti per certificare i nostri servizi in base a questo standard.

Una copia del rapporto più recente è disponibile su richiesta presso il tuo account manager o rappresentante commerciale.

SOC 3
A differenza di un rapporto SOC 2, un report SOC 3 può essere distribuito al pubblico per uso generale. Siamo stati sottoposti a una verifica di terze parti per certificare i nostri servizi in base a questo standard.

Per visualizzare il nostro rapporto SOC 3, **fai clic qui**.

HITRUST
La nostra soluzione video ha ottenuto lo stato di Certificato per la sicurezza delle informazioni da parte di HITRUST. Lo stato di certificazione di HITRUST CSF indica che abbiamo soddisfatto i requisiti di sicurezza definiti da HITRUST e che stiamo gestendo in modo appropriato il rischio per la sicurezza informatica.

HIPAA
Per servire meglio i nostri clienti del settore sanitario, sottoposto a rigorosa regolamentazione, abbiamo implementato misure di protezione della sicurezza HIPAA. Ogni anno veniamo sottoposti a una verifica SOC 2+ di terze parti, che consiste in una valutazione dei controlli mappati in base ai requisiti della Regola di sicurezza HIPAA, che dimostra l'implementazione delle misure di sicurezza e dei requisiti di cui alla normativa sulla sicurezza HIPAA. Alle entità interessate offriamo accordi societari HIPAA per Business Associate. Una copia del rapporto più recente è disponibile su richiesta presso il tuo account manager o rappresentante commerciale.

Programma CloudTrust di McAfee
Abbiamo ottenuto la valutazione Enterprise-Ready di McAfee CloudTrust, la più alta possibile. McAfee conferisce questo stato ai servizi cloud che soddisfano appieno i requisiti più rigorosi di protezione dei dati, verifica dell'identità, sicurezza dei servizi, prassi aziendali e tutela legale.

Regolamento generale sulla protezione dei dati (GDPR)
Forniamo ai clienti un dettagliato Accordo sul trattamento dei dati (DPA) che regola il rapporto tra il cliente e Avaya Cloud Office. Il nostro DPA contiene efficaci impegni sulla privacy che poche aziende di software possono eguagliare ed è stato aggiornato per confermare la nostra conformità con il GDPR.

Conclusione

Per noi, la sicurezza è una componente fondamentale delle comunicazioni interne ed esterne di ogni organizzazione. Pertanto, ci impegniamo a garantire ai clienti i massimi livelli di integrità, riservatezza, conformità e controllo.

Facendo leva su una solida infrastruttura back-end e un team globale addetto alla sicurezza, il nostro approccio multilivello alla sicurezza, incentrato su più discipline che spaziano dallo sviluppo di software ai controlli degli accessi, assicura che i dati e le comunicazioni dei clienti siano tutelati in ogni fase. In questo modo, non solo la tua attività è protetta dagli attacchi, ma il tuo reparto IT può anche concentrarsi sulle funzioni aziendali piuttosto che sulla sicurezza delle applicazioni.

Le organizzazioni di oggi hanno bisogno di provider di tecnologia che migliorino continuamente le loro funzionalità di sicurezza, garantendo servizi di primo livello. Siamo orgogliosi di essere uno di quei fornitori e cerchiamo di mettere a disposizione la nostra competenza per aiutare i nostri clienti a soddisfare le loro esigenze aziendali pur restando impegnati a garantire loro i massimi livelli di sicurezza, riservatezza dei dati, conformità, disponibilità e controllo.

Informazioni su Avaya

Le aziende nascono dalle esperienze che offrono, e ogni giorno Avaya offre milioni di esperienze (NYSE:AVYA). Per oltre un secolo, abbiamo consentito alle organizzazioni di tutto il mondo di avere successo, creando esperienze di comunicazione intelligenti per clienti e dipendenti. Avaya fornisce soluzioni aperte, convergenti ed innovative per migliorare e semplificare le comunicazioni e la collaborazione, in modalità cloud, locale o ibrida. Per far crescere la tua azienda, siamo impegnati su Innovazione e Partnership come elementi strategici fondamentali per proiettarci con successo nel futuro. Siamo l'azienda tecnologica alla quale puoi affidarti per offrire esperienze che contano. Visita il nostro sito www.avaya.com/it

AVAYA | Experiences That Matter

11/20 • CL15481IT