CITRIX®

White paper

Linee guida per garantire la business continuity per la vostra organizzazione

Mettete la vostra azienda al riparo dalle interruzioni e garantite la produttività della vostra forza lavoro.

Questo white paper propone un approccio completo per far sì che le persone restino produttive sia durante le interruzioni programmate sia durante quelle non pianificate. Include le best practice per una strategia completa di business continuity, così come le tecnologie per fornire l'accesso sicuro alle applicazioni e ai dati su qualsiasi dispositivo, tramite qualsiasi rete o cloud. Garantendo la continuità delle operazioni a prescindere dagli eventi avversi, le soluzioni Citrix Workspace vi aiutano a proteggere l'azienda da conseguenze negative come perdite economiche, danni alla reputazione, fratture nei rapporti con i partner e i clienti, e cali di produttività.

Ogni organizzazione deve affrontare la possibilità di interruzioni più o meno gravi: dagli eventi pianificati, come manutenzione IT e cambi di sede, alle emergenze come uragani, tempeste di neve ed epidemie, fino a eventi imprevisti che colpiscono senza alcun preavviso, come terremoti, tornado, attacchi terroristici e incendi. Anche incidenti relativamente minori come guasti alla rete idrica, cali di tensione, ritardi dovuti al traffico e malanni stagionali possono avere un impatto significativo.

Sebbene la pianificazione della business continuity si sia tradizionalmente concentrata sulla pianificazione del failover e dell'elevata disponibilità dei sistemi aziendali mission-critical, questa è solo una parte del quadro generale. Per mantenere a regime l'azienda, le organizzazioni devono adottare un approccio di più ampio respiro che includa sia misure a livello organizzativo, sia tecnologie in grado di ridurre al minimo le interruzioni, garantire la sicurezza e sostenere una produttività ininterrotta per gli utenti e i team. Le best practice per una strategia di business continuity completa dovrebbero contemplare aspetti come la struttura del team di business continuity, la pianificazione della business continuity, i test di disaster recovery e business continuity, la comunicazione in situazioni di crisi e i programmi di sicurezza e sensibilizzazione dei dipendenti.

Fornendo agli utenti l'esperienza di cui necessitano, un workspace digitale sicuro può garantire un accesso ottimizzato alle applicazioni e ai dati aziendali su ogni dispositivo e tramite qualsiasi rete, con hosting in locale o su un cloud pubblico. La consapevolezza contestuale consente di raggiungere il giusto livello di sicurezza e flessibilità per la loro situazione attuale, senza compromettere le risorse aziendali. I sistemi di analytics e insight possono aiutare il reparto IT a garantire la sicurezza, la conformità e la protezione dalle minacce, a prescindere da dove e come lavorino le persone.

L'importanza della business continuity e le sfide che essa pone

Che siano pianificate o meno, le interruzioni dell'attività che non vengono gestite in modo efficace hanno un costo elevato. Perdite di fatturato, opportunità di vendita mancate e contratti di servizio non rispettati possono avere un impatto economico devastante. Le interruzioni nelle relazioni con i partner e nelle catene di fornitura possono ritardare il time-to-market, ostacolare iniziative importanti e indebolire il vantaggio competitivo. Una risposta inadeguata può danneggiare l'immagine pubblica dell'azienda, così come la fiducia dei suoi clienti e investitori. Dopo l'interruzione, le persone possono avere difficoltà a tornare pienamente produttive a causa di perdite di dati, lavori in corso interrotti e la perdita di coesione collaborativa con il resto del team e la dirigenza, per non parlare dell'impatto personale che l'evento può aver avuto su di loro.

“La sicurezza e la protezione dei nostri studenti, del nostro personale e della nostra comunità sono di fondamentale importanza. Per consentire al nostro personale di fornire la didattica di alta qualità per cui l’Università di Sydney è rinomata, dobbiamo affidarci a una tecnologia che ci consenta di facilitare la condivisione e la fruizione della conoscenza in modi sicuri e protetti.”

Jordan Catling | Associate Director, Client Technology ICT | Università di Sydney

Per il reparto IT, riprendersi da un’interruzione dell’attività può essere un processo lungo e complesso che richiede di:

- Riportare online il datacenter e ripristinare tutti i dati persi
- Sostituire i dispositivi persi o inaccessibili e garantire che ciascuno sia in grado di eseguire il software richiesto dall’utente
- Effettuare il provisioning e la configurazione delle applicazioni
- Progettare nuovi modi di lavorare, dai metodi alternativi di accesso alla rete alle soluzioni per le applicazioni che non sono più accessibili, e comunicarli agli utenti
- Svolgere tutte queste operazioni nel bel mezzo di una situazione di emergenza

Un piano di business continuity efficace semplifica e accelera notevolmente questo processo, aiutando il reparto IT a ripristinare e mantenere il servizio dell’organizzazione, facendo in modo che le persone tornino al lavoro il più velocemente possibile. Negli eventi ove si dispone di un certo preavviso, come un cambio di sede programmato o un’emergenza meteo anticipata, l’organizzazione può perfino impedire del tutto che il lavoro venga interrotto.

Un approccio globale alla vostra strategia di business continuity

Sebbene ogni emergenza sia unica e molte decisioni debbano sempre essere prese sul momento, un piano di business continuity fornisce un framework e la preparazione necessari a guidare tali decisioni, così come una chiara indicazione su chi debba prenderle. Affinché i programmi di business continuity abbiano successo, è necessario che gli executive giochino un ruolo attivo nello sviluppo di tali piani e si assicurino il sostegno di tutti gli altri dirigenti aziendali. Con questo sostegno, i reparti IT e quelli impegnati nella sicurezza possono promuovere lo sviluppo di una strategia di business continuity globale che comprenda tutti i seguenti elementi essenziali.

“Per quanto possibile, ci siamo sforzati di uniformare l’esperienza [dei dipendenti], così che ora non ha importanza se sono in ufficio o a casa propria, in hotel o a bordo di un aereo: sotto il profilo del linguaggio, del funzionamento e della grafica, il loro dispositivo è quanto più vicino possibile al loro desktop.”

Sarah Vogt | Remote Systems Engineer
Greenberg Traurig, LLC

Standard di business continuity di Citrix

Struttura del team

Una delle considerazioni più importanti per un piano di business continuity è lo sviluppo di una chiara gerarchia decisionale. In situazione di emergenza, il personale non dovrebbe perdere tempo a domandarsi chi abbia la responsabilità o l’autorità di prendere una determinata decisione.

L’organizzazione dovrebbe essere in grado di affrontare tutte le attività di business continuity in ogni luogo in cui opera, sia per rispondere agli eventi locali, sia per coordinare la risposta di tutta l’azienda alle emergenze locali e più generali. I responsabili principali del team di business continuity devono rimanere coinvolti nella pianificazione e nei test durante tutto l’anno per garantire che il piano sia efficace e aggiornato, oltre che per acquisire la familiarità necessaria con le procedure da seguire nel caso di un’emergenza reale.

In Citrix, un team di business continuity di base per ogni regione comprende: dirigenti, reparto IT, strutture e risorse immobiliari, così come sicurezza fisica, comunicazioni, risorse umane, finanza e altri reparti. I singoli team sono dedicati a:

- **Risposta alle emergenze:** guida le attività di pianificazione della business continuity; fornisce raccomandazioni finali al comitato esecutivo di gestione; fornisce indicazioni generali per la preparazione, la risposta e il recupero
- **Comunicazioni:** gestisce la comunicazione con tutte le parti, compresi dipendenti, fornitori, agenzie di servizi pubblici e clienti
- **Risposta del campus:** prepara le strutture e le attrezzature per l’evento disastroso imminente; esegue l’assessment post-evento del danno e del suo impatto sulle operazioni in corso; fornisce assistenza con le richieste di indennizzo; mette in sicurezza edifici e terreni

- **Preparazione aziendale:** funge da collegamento con i team delle singole unità aziendali; adotta le misure necessarie per attuare le operazioni aziendali di emergenza per ciascuna unità; fornisce una risposta e una direzione aziendale tattica

Ognuno di questi team rende conto al comitato esecutivo di gestione di Citrix.

Pianificazione della business continuity

A un livello elevato, un piano di business continuity dovrebbe identificare sia le potenziali interruzioni di business che possono colpire qualsiasi sede dell'organizzazione, come interruzioni di corrente, epidemie, pandemie, e incendi, sia quelle limitate a determinati luoghi, come terremoti e tsunami in una regione ad alto rischio sismico o disordini civili nelle aree politicamente instabili. La pianificazione si estende anche lungo l'intera catena di approvvigionamento, compresa la revisione delle strategie di business continuity per i principali fornitori, l'identificazione dei potenziali rischi di interruzioni operative e la valutazione delle alternative. Per mantenere gestibile il numero di scenari, la pianificazione dovrebbe basarsi sugli scenari peggiori, anziché su più versioni di varia intensità di ciascun incidente.

"Vogliamo arrivare al punto in cui i dipendenti comprendano che tutto ciò di cui hanno bisogno per svolgere il proprio lavoro può essere raggiunto tramite Citrix."

Kyle Edgeworth | Deputy CIO Città di Corona

Non sempre è possibile mantenere la normale operatività in una situazione di emergenza. Per limitare l'impatto della riduzione di capacità, il team dovrebbe stabilire quali operazioni sono più importanti, chi le eseguirà e come verrà reindirizzato il lavoro in caso di necessità. In Citrix questo aspetto viene gestito da un team di responsabili di unità aziendali dotato di un analista della business continuity. Questo gruppo collabora per valutare la criticità dei diversi processi aziendali in termini di fatturato, questioni orientate al cliente e immagine del marchio, implicazioni normative e altre considerazioni aziendali, per poi associare le dipendenze a questi processi in base alle applicazioni, persone, strutture e attrezzature necessarie per supportarli. In base a questa analisi, il gruppo può individuare le strategie e i costi di ripristino per recuperare ogni processo. Per l'IT, questi dati forniscono un framework per garantire che le applicazioni fondamentali siano disponibili entro gli obiettivi relativi al tempo di recupero (RTO) e al punto di recupero (RPO) stabiliti.

Test

Un piano di business continuity è efficace solo se lo si rispetta. In un momento di emergenza, un'organizzazione che non pone un'attenzione costante alla preparazione può rendersi conto che il piano d'azione non è più adeguato alla propria attività o alle proprie operazioni. Essa si troverà così costretta a reagire con una risposta ad hoc dettata dalla nuova circostanza che, proprio per il suo carattere di emergenza, viene penalizzata da un falso senso di sicurezza.

Le best practice richiedono che gli aggiornamenti annuali di un piano di business continuity riflettano i cambiamenti nella criticità e dipendenza delle applicazioni, le priorità aziendali, la gestione del rischio, le sedi aziendali, le operazioni e altro ancora. In Citrix, il personale addetto alla business continuity monitora e prende nota di tali cambiamenti nel corso dell'anno per completare la revisione annuale. Almeno una volta all'anno, dovrebbero essere effettuate anche simulazioni di emergenza complete. Queste linee guida dovrebbero essere considerate come

un requisito minimo, in aggiunta a una revisione annuale di tutti i piani, così come di test di comunicazione in situazioni di crisi. Citrix conduce test trimestrali di business continuity e di ripristino per tutte le applicazioni mission-critical. Gli esercizi di simulazione servono a introdurre nuovi sviluppi per garantire la flessibilità dei piani vigenti e abituare il team a rispondere agli imprevisti.

Comunicazione in situazioni di crisi

Un programma prestabilito di comunicazione in situazioni di crisi può fare la differenza fra una risposta all'emergenza organizzata e una frettolosa. Il piano deve identificare tutti i soggetti interessati dalle comunicazioni di emergenza, compresi dipendenti, collaboratori temporanei, clienti, fornitori, media e dirigenti. Il set di strumenti di comunicazione dell'organizzazione dovrebbe includere risorse interne ed esterne, quali telecomunicazioni, e-mail, indirizzo pubblico, intranet, IM, SMS e il sito web dell'azienda. Il team di comunicazione dovrebbe impegnarsi per trasmettere un messaggio coerente a nome dell'azienda attraverso canali esterni quali comunicati stampa, aggiornamenti sui social media e interviste con i portavoce. È possibile redigere in anticipo esempi di messaggi di emergenza, adattati per tipi di pubblico e modalità di comunicazione specifici, che possano essere aggiornati rapidamente durante un'emergenza reale in base alle condizioni del momento.

Sicurezza dei dipendenti

Tenere al sicuro le persone dovrebbe essere la priorità assoluta in qualsiasi risposta alle emergenze. Ci sono molti modi per sviluppare un programma di sicurezza dei dipendenti. Agenzie locali come la Croce Rossa, i vigili del fuoco, il dipartimento di polizia e gli enti federali, come i Community Emergency Response Teams (CERT) della FEMA negli Stati Uniti, possono offrire un training per la gestione delle emergenze e altre indicazioni per il vostro programma. Gli esercizi di simulazione possono aiutare a sviluppare e perfezionare le procedure più adeguate per i dipendenti, le strutture e le sedi di lavoro. Una volta completato, il programma dovrebbe essere incluso nell'orientamento dei nuovi dipendenti e rivisto regolarmente con tutti i dipendenti. Le procedure di evacuazione di emergenza devono essere riviste e verificate di frequente, e i dipendenti devono sempre sapere dove trovare la documentazione sulla business continuity. Durante un'emergenza, prestate attenzione ai livelli di stress delle persone e assicuratevi che abbiano tutto il tempo necessario per dormire, mangiare e rilassarsi.

Tabella 1	Lista di controllo per la pianificazione della business continuity
Struttura del team di business continuity	Assicurarsi il sostegno dei dirigenti Formare un team di business continuity di base
Pianificazione della business continuity	Creare un team di analisi aziendale Sviluppare scenari di emergenza Definire le gerarchie decisionali Dare priorità al ripristino in base alle considerazioni aziendali Associare gli obiettivi di ripristino alle dipendenze Sviluppare una strategia di continuità per il datacenter Sviluppare una strategia di continuità per la forza lavoro Considerare una scalabilità orizzontale/verticale, in base alla gravità della situazione
Test di disaster recovery e business continuity	Aggiornare regolarmente i piani* Verificare la recuperabilità delle applicazioni mission-critical* Svolgere esercizi di simulazione e procedure dettagliate*
Comunicazione in situazioni di crisi Programmi di sicurezza e sensibilizzazione dei dipendenti	Stabilire un programma formale di comunicazione in situazioni di crisi Identificare i soggetti interessati dalle comunicazioni di emergenza Identificare i principali canali di comunicazione interni Redigere esempi di comunicazioni Sviluppare programmi attraverso esercizi di simulazione e formazione sulla risposta alle emergenze da parte delle agenzie locali Integrare la sicurezza e la sensibilizzazione nell'orientamento dei nuovi dipendenti Rivedere e verificare le procedure di evacuazione di emergenza

Continuità della forza lavoro: consentire l'accesso ininterrotto alle risorse aziendali

Un'infrastruttura dal design a elevata disponibilità, distribuita in locale e sul cloud, può consentire al reparto IT di svolgere le proprie attività. Tuttavia, se le persone sono state allontanate dal loro solito luogo di lavoro o se hanno perso l'accesso ai loro dispositivi o sistemi consueti, cosa si può fare? Un programma di business continuity efficace e completo deve contemplare non solo il datacenter ma anche la forza lavoro. In poche parole, se le persone non possono svolgere il proprio lavoro, l'azienda non può funzionare.

Sebbene la business continuity abbia tradizionalmente previsto la designazione di un luogo di lavoro alternativo o di un'unità di recupero, le organizzazioni utilizzano sempre più strumenti di mobility aziendale per consentire alle persone di lavorare dove è più comodo ed efficace. Coloro che si trovano a lavorare proprio nel luogo dell'evento disastroso, come il team di business continuity, gli addetti alla risposta alle emergenze, gli addetti a servizi critici e altri, come i periti assicurativi, possono essere ospitati in qualsiasi struttura o unità mobile disponibile, senza la necessità di infrastrutture speciali o di una connettività complessa.

In Citrix, la stessa tecnologia impiegata per i workspace digitali sicuri consente alle persone di collegarsi con le applicazioni e i dati sia nelle operazioni di routine sia nelle situazioni di emergenza, utilizzando qualsiasi dispositivo, rete o cloud. Ciò consente alle persone di occuparsi di qualsiasi priorità in tutta semplicità, che si tratti di continuare a lavorare normalmente, svolgere nuovi compiti richiesti dall'evento, o concentrarsi sui propri bisogni e su quelli delle proprie famiglie, per poi riprendere il lavoro in funzione

delle circostanze. Invece di dovere acquistare PC che soddisfano determinate specifiche, configurarli, fornire l'accesso alle applicazioni e così via, possiamo chiudere un ufficio, spostare le persone in un'altra sede e farle tornare a lavorare rapidamente nell'ambiente che conoscono meglio. Questo consente di fornire la medesima esperienza utente. D'altro canto, il reparto IT non deve preoccuparsi di creare un'immagine di decine o centinaia di macchine, per poi guidare le persone attraverso una lunga serie di processi modificati.

Questo approccio offre vantaggi importanti, fra cui:

Efficienza e risparmio. Rendere la mobility e l'accesso remoto elementi centrali nella pianificazione della business continuity consente di aumentare il valore di questi investimenti, eliminando molti processi e costi di business continuity separati.

Un'esperienza ottimizzata per le persone. Poiché le persone accedono e utilizzano le loro risorse sempre allo stesso modo e con la stessa esperienza di workspace digitale sicuro in qualsiasi situazione, non vi è alcuna necessità di procedure alternative da imparare o ricordare.

Sicurezza e conformità. Durante un evento di business continuity, i dati e le applicazioni sono distribuiti usando la stessa infrastruttura utilizzata per le normali operazioni, con la stessa sicurezza intrinseca. Le applicazioni Windows rimangono sotto il controllo del reparto IT nell'infrastruttura cloud ibrida, dove l'automazione e la gestione centralizzata migliorano l'applicazione delle policy, la conformità normativa e la protezione antivirus. Analogamente, gli utenti possono accedere in modo sicuro alle applicazioni e ai dati aziendali sensibili, da qualsiasi dispositivo e da ogni luogo, garantendo al contempo al reparto IT una capacità completa di controllo, tracciabilità, reporting e verificabilità a supporto della sicurezza e della conformità. I dati distribuiti ai dispositivi mobile sono protetti e controllati attraverso la gestione dei dispositivi mobile (MDM), mentre le applicazioni sono protette e controllate attraverso la gestione delle applicazioni mobile (MAM). La crittografia end-to-end fornisce un ulteriore livello di protezione in quanto le persone accedono alle applicazioni e ai dati aziendali tramite qualsiasi rete, da ogni luogo.

Un'esecuzione più pratica e a basso rischio. Le organizzazioni possono avvalersi del piano di business continuity con meno disagi per gli utenti e per l'azienda. Come risultato, l'organizzazione è spesso più disposta a prendere questa misura in modo proattivo (ovvero spostare fuori sede le persone prima di un uragano o di una tempesta di neve, o farle lavorare da casa durante un'epidemia o perfino evacuare verso una città diversa nel caso di una imminente interruzione su larga scala), piuttosto che correre rischi nella speranza che la situazione avversa passi senza conseguenze negative sull'azienda. Il piano diventa molto più efficace quando è visto come un adeguamento accettabile alle circostanze piuttosto che come ultima istanza di cui avvalersi solo nei momenti più disperati, o all'ultimo momento.

Citrix, con sede a Fort Lauderdale, in Florida, ha una vasta esperienza diretta negli eventi di business continuity. Citrix ha trasferito il personale nelle sale conferenze degli hotel, ha distribuito i carichi di lavoro in tutto il mondo a causa di strutture chiuse, e ha aumentato rapidamente la capacità in altre aree in caso di potenziali

disastri. Citrix l'ha fatto molte volte, specialmente durante la stagione degli uragani in Florida. I servizi forniti internamente ed esternamente ai clienti non ne hanno mai risentito, grazie alla flessibilità della forza lavoro permessa dalle tecnologie Citrix.

Garantire la continuità della forza lavoro con le tecnologie Citrix

Con un workspace digitale sicuro, Citrix aiuta le organizzazioni a garantire la continuità delle operazioni durante le interruzioni dell'attività aziendale. Le soluzioni di Citrix Workspace leader del settore consentono al reparto IT di fornire in modo sicuro tutte le applicazioni (Windows, web, SaaS e mobile) così come i dati e i servizi da qualsiasi dispositivo, su qualsiasi rete o cloud. Citrix supporta la continuità della forza lavoro, grazie a tecnologie complete che semplificano le operazioni di sicurezza e riducono i rischi nelle seguenti aree principali.

Accesso contestuale

Anziché preoccuparsi di metodi di accesso speciali, il reparto IT può consentire alle persone di accedere al proprio workspace digitale sicuro nel solito modo con qualsiasi connessione disponibile. Gli utenti possono collegarsi tramite la LAN o la WAN aziendale, la banda larga personale, le connessioni satellitari, tramite hotspot pubblico o mobile, con le stesse funzionalità complete di sicurezza, controllo degli accessi, monitoraggio e tracciabilità della conformità. Citrix Gateway (in precedenza NetScaler Gateway) fornisce un framework di gestione unificato affinché il reparto IT possa proteggere, controllare e ottimizzare l'accesso ad applicazioni e dati su qualsiasi dispositivo, utilizzando qualsiasi rete o cloud.

Le persone che non dispongono più dell'accesso al proprio dispositivo di lavoro abituale possono collegarsi tramite qualsiasi dispositivo al proprio workspace digitale sicuro, dove troveranno tutte le applicazioni di lavoro che utilizzano quotidianamente. Potete scaricare la Workspace App su tutti i nuovi dispositivi acquistati o su un vecchio dispositivo personale, tra cui desktop e laptop Windows e Mac, dispositivi mobile iOS, Android e Windows nonché Google Chromebook. All'interno di Citrix Workspace, gli utenti disporranno dell'accesso con un solo clic alle applicazioni aziendali mobile, web, SaaS, personalizzate e Windows, incluse applicazioni integrate per la condivisione di file e per la produttività.

Sicurezza delle applicazioni

La virtualizzazione del desktop e delle applicazioni Windows powered by Citrix Virtual Apps and Desktops (in precedenza XenApp e XenDesktop) consente all'IT di trasformare le applicazioni e i desktop completi Windows in servizi on-demand distribuiti in modo sicuro a workspace digitali su qualsiasi dispositivo e in qualsiasi luogo. Poiché le applicazioni e i dati sono gestiti all'interno del datacenter o del cloud, il reparto IT mantiene capacità centralizzate di protezione dei dati, conformità, controllo degli accessi e amministrazione degli utenti, con la stessa facilità sui dispositivi personali, presi in prestito o appena acquistati e sugli endpoint di proprietà aziendale, all'interno di un medesimo ambiente unificato.

I dispositivi mobile possono giocare un ruolo particolarmente importante nel mantenere gli utenti connessi con l'azienda in caso di interruzioni. Citrix Endpoint Management (in precedenza XenMobile) consente il provisioning e il controllo di applicazioni, dati e dispositivi basato sull'identità, nonché il deprovisioning automatico dell'account e la cancellazione selettiva di qualsiasi dispositivo utilizzato temporaneamente durante un evento di business continuity.

Le applicazioni e i dati aziendali, sviluppati dall'IT o da terze parti, e le applicazioni di produttività mobile di livello enterprise incluse, rimangono in un container, separati dalle applicazioni e dai dati personali presenti sul dispositivo.

Sicurezza dei dati

Citrix Content Collaboration (in precedenza ShareFile) consente agli utenti, ai team e ai clienti di accedere, sincronizzare e condividere in modo sicuro i file da qualsiasi luogo, su ogni dispositivo. Il reparto IT può fornire, con facilità, l'accesso ai repository di dati aziendali esistenti, senza compromettere la sicurezza. I consueti flussi di lavoro dei documenti, come le procedure di approvazione, possono essere automatizzati per garantire la continuità dei processi aziendali anche in circostanze insolite. Vari aspetti contribuiscono a mantenere sicuri i contenuti aziendali in caso di interruzioni dell'attività: opzioni di storage flessibili, controllo basato sulle policy, reporting, crittografia dei dati, cancellazione remota, supporto IRM (information rights management) e integrazione di sistemi DLP (data loss prevention).

Insieme, queste tecnologie Citrix aiutano i pianificatori della business continuity a rispondere alle due domande essenziali per gli utenti:

- Posso ancora accedere ad applicazioni, dati e file e collaborare efficacemente con altri soggetti all'interno e all'esterno dell'organizzazione?
- Funziona tutto ancora allo stesso modo o devo adeguarmi a un dispositivo, un metodo di accesso alla rete e un insieme di strumenti sconosciuti?

Continuità del datacenter: garantire la continuità delle attività del reparto IT

La maggior parte delle grandi organizzazioni ha già adottato un modello di cloud ibrido e hanno più di un datacenter; al contempo sfruttano il cloud per questioni di scalabilità e ridondanza. Se un datacenter o cloud va offline per un qualsiasi motivo, previsto o imprevisto, le persone dovrebbero essere in grado di accedere alle risorse attraverso un altro datacenter o tramite risorse sul cloud, che siano attive o di backup, fino a quando il datacenter o il cloud interessati tornano online. È importante assicurarsi che l'infrastruttura associata sia in grado di supportare questa risposta, dal failover rapido e automatizzato al bilanciamento del carico e alla capacità della rete.

Le organizzazioni basate sui PC desktop tradizionali per l'accesso primario ai dati e alle risorse si trovano spesso in una posizione di svantaggio quando devono fronteggiare eventi imprevisti. Con l'accesso da remoto ai PC fornito da Citrix, i clienti Citrix Virtual Apps and Desktops possono fornire rapidamente l'accesso a singole macchine all'interno del luogo di lavoro fisico. In caso di evento imprevisto, gli amministratori possono distribuire rapidamente un pacchetto MSI ai PC desktop e fornire agli utenti l'accesso sicuro a tali dispositivi da qualsiasi luogo.

Continuità degli utenti

La condizione auspicabile è che il reparto IT abbia distribuito una soluzione che offra all'utente finale la medesima esperienza a prescindere dal luogo fisico. Grazie alle funzionalità intelligenti, Citrix Workspace espande la capacità degli utenti di essere produttivi ovunque si trovino. Disponendo di un feed intelligente

di attività su qualsiasi dispositivo, le persone possono continuare a lavorare anche in periodi di incertezza.

Sicurezza della rete

Citrix ADC (in precedenza NetScaler ADC) e Citrix SD-WAN (in precedenza NetScaler SD-WAN) ottimizzano il failover del datacenter per gli utenti. Se il datacenter primario diventa inattivo, Citrix ADC reindirizza gli utenti in modo automatico e trasparente al sito secondario, proseguendo al contempo le operazioni di bilanciamento del carico e di bilanciamento del carico globale. Inoltre, Citrix ADC permette alle organizzazioni che utilizzano un cloud pubblico per il backup di gestire questa infrastruttura esterna nello stesso modo in cui utilizzerebbero il proprio datacenter di backup. Citrix SD-WAN consente al reparto IT di collegare e accelerare le applicazioni, ottimizzare l'utilizzo della larghezza di banda fra cloud pubblici di terze parti e reti private, nonché ottenere visibilità sulla prestazione delle applicazioni per ottimizzare l'esperienza utente in qualsiasi situazione.

Automazione e recupero

Le soluzioni Citrix aiutano il reparto IT a garantire che le risorse del datacenter rimangano disponibili. Citrix Hypervisor (in precedenza XenServer), la piattaforma leader del settore per la virtualizzazione cloud, server e desktop economicamente efficiente, fornisce gli strumenti per la gestione completa del disaster recovery a livello di sito, tra cui la migrazione in tempo reale dei carichi di lavoro da un server fisico ad un altro. Inoltre, offre un'elevata disponibilità automatizzata, che ridistribuisce le macchine virtuali da un host che non è operativo ad altri host fisici, riavviandoli per proteggere carichi di lavoro critici da eventi localizzati.

I servizi Citrix Cloud promuovono la resilienza fornendo al reparto IT un singolo dashboard per gestire le risorse distribuite in vari datacenter aziendali e cloud pubblici e privati. Il reparto IT può riassegnare gli utenti a siti alternativi in base alla necessità per ridurre il carico su risorse messe a dura prova e al contempo garantire la disponibilità e le prestazioni. I servizi Citrix Cloud vengono eseguiti tramite una piattaforma distribuita a livello globale e dall'elevata disponibilità, progettata per garantire la continuità operativa a prescindere dalle interruzioni locali.

Analytics e insight

In una situazione di business continuity, la distribuzione degli utenti e dei carichi di lavoro attraverso l'infrastruttura di rete può essere notevolmente alterata, rendendo particolarmente importante il monitoraggio delle prestazioni per garantire un'esperienza di buon livello a ogni utente. Al contempo, il reparto IT resta in allerta per evitare minacce alla sicurezza in modo che le interruzioni verificatesi non creino opportunità per gli hacker. Le soluzioni offerte da Citrix, come Citrix ADC, Citrix Application Delivery Management (in precedenza NetScaler Management and Analytics System), e Citrix Virtual Apps and Desktops vi forniscono una visibilità completa sulla vostra infrastruttura IT, con analytics in tempo reale per rilevare minacce, configurazioni errate e problematiche di prestazioni.

Citrix Analytics for Performance e Citrix Analytics for Security offrono insight in tempo reale e azionabili per garantire che le attività nel vostro ambiente procedano senza interruzioni. Grazie alle informazioni dettagliate sull'esperienza di ciascun utente, il reparto IT è in grado di offrire maggiori risorse a una persona che sta riscontrando prestazioni non ottimali.

Conclusioni

L'essenza della business continuity consiste nel minimizzare l'impatto che le interruzioni possono avere sulle persone e sulle risorse IT su cui fanno affidamento. In passato, le organizzazioni hanno dovuto fare affidamento su metodi di lavoro alternativi e su postazioni alternative in tali situazioni, costringendo le persone a adattarsi a modi insoliti di lavorare, proprio mentre si trovavano ad affrontare lo stress e l'incertezza dell'evento stesso. Citrix supporta un approccio olistico e ottimizzato, consentendo alle persone di lavorare esattamente allo stesso modo durante un'emergenza, come se si trattasse di qualsiasi altro giorno. Oltre che ad aiutare il reparto IT a garantire un livello di sicurezza e controllo privo di interruzioni, una gamma completa di tecnologie per l'accesso contestuale alla rete, nonché per la sicurezza delle applicazioni e dei dati consente alle persone di essere totalmente produttive su qualsiasi dispositivo, su ogni rete o cloud e in qualsiasi luogo. A livello di back-end, l'automazione e il ripristino garantiscono che le risorse IT locali restino disponibili, mentre il monitoraggio, il rilevamento e l'analytics in tempo reale consentono al reparto IT di assicurare una buona esperienza utente, di garantire la conformità e di prevenire le violazioni alla sicurezza. Sfruttando l'infrastruttura usuale, questo approccio elimina anche la necessità di un accesso a strumenti e dispositivi separati per la business continuity, riducendo il costo e la complessità della relativa pianificazione.

I workspace digitali sicuri stanno trasformando il modo in cui le organizzazioni IT di tutto il mondo agevolano gli utenti e supportano le aziende. Integrando le soluzioni Citrix nella vostra strategia di business continuity, potete proteggere la vostra organizzazione in modo di gran lunga più efficace contro i rischi derivanti da interruzioni pianificate e impreviste.

Per maggiori informazioni, visitate la pagina https://www.citrix.it/virtual-apps.