

Virtualizzazione e sicurezza il valore della tecnologia

SICUREZZA E VIRTUALIZZAZIONE: L'EQUILIBRIO TRA VELOCITÀ, FLESSIBILITÀ E CONTROLLO

- Il fenomeno della virtualizzazione nei sistemi distribuiti è ormai considerato uno standard *de-facto*, maturo e universalmente accettato per gli evidenti vantaggi in flessibilità nelle operazioni IT e per la riduzione degli investimenti in nuovo hardware. La pervasività degli ambienti virtualizzati è apprezzata nell'ambito dello sviluppo come in quello della produzione: il segmento aziendale dedicato allo sviluppo software può beneficiare di un fattore critico per realizzare rapidamente ambienti adatti alla costruzione e al collaudo funzionale di moduli software, mentre la linea IT assegnata alla produzione è in grado di contenere i costi di hardware e software grazie alla capacità di sintetizzare funzionalità anche complesse in *immagini replicabili* e indipendenti dalla loro collocazione fisica, gestendo il data center in *flessibilità*.

Eppure, non è raro scoprire che le policy di sicurezza presenti negli ambienti di sviluppo e di collaudo sono disallineate rispetto alle aree di produzione e di erogazione dei servizi IT. E, anche se i sistemi di produzione sono dotati di



Gabriele Provinciali
senior solution architect, CA Technologies

sofisticate tecnologie di comando e controllo e di regole di sicurezza particolarmente stringenti, i responsabili dei sistemi informativi fanno ancora fatica a estendere e propagare regole e procedure, pensate precedentemente per i sistemi fisici, ai sistemi virtualizzati. I vantaggi tecnologici forniti dalle tecniche di virtualizzazione, *velocità* e *flessibilità*, non sono sempre accompagnati dal *controllo* in termini di sicurezza che abitualmente è presente nei classici ambienti business-critical. Quali

sono le ragioni di questa difficoltà e quali sono gli strumenti per riportare in equilibrio, e in conformità, le componenti virtuali dei servizi IT presenti nelle imprese?

GLI AMBIENTI IT DI PRODUZIONE: ESTENDERE LA SICUREZZA AI SISTEMI VIRTUALIZZATI

- La transizione dalla pura flessibilità alla *flessibilità mediata dal controllo*, negli ambienti IT di produzione, è già cominciata da qualche tempo: le iniziative a carico dell'IT aziendale sono diverse e

hanno gradienti di difficoltà che spaziano dalla disponibilità di fondi per l'implementazione alla complessità di gestione dovuta ad ambienti eterogenei, passando per una mancanza di competenze interne e/o di procedure adeguate agli standard presenti in azienda. Questi freni inibitori, però, non fanno distogliere l'attenzione dal problema di fondo: l'assoluta maggioranza dei responsabili IT di tutti i settori è convinta che la questione della sicurezza debba essere risolta attraverso una gestione unificata e coerente di ambienti fisici e virtuali per proteggere dati sensibili, mantenere la conformità alle normati-

ve e governare il fenomeno del *virtual sprawling*, ovvero la disseminazione incontrollata di istanze virtuali che possono sfuggire ai controlli di sicurezza, di gestione delle licenze software, di compatibilità con le regole aziendali. Una delle risposte più apprezzate per la risoluzione di questi problemi? *L'automazione*, che sembra essere l'unica arma affilata per una stretta integrazione tra infrastruttura e sicurezza come *servizio aziendale*, esteso dai sistemi fisici a quelli virtualizzati.

SICUREZZA E VIRTUALIZZAZIONE: LE AREE CRITICHE

- Il governo dei sistemi IT predilige un'infrastruttura e strumenti *unificati* per la gestione della sicurezza dei propri ambienti informativi. Le aree sulle quali i responsabili dei sistemi informativi sono in grado di investire per garantire l'estensione e il miglioramento della sicurezza già presente negli ambienti di produzione, riguardano diversi segmenti tecnologici, che vanno dall'automazione, alla gestione delle prestazioni, alla gestione strutturata delle anomalie.

La **gestione delle configurazioni** (*change e configuration management*), da sempre elemento critico nel data center, assume una valenza fondamentale per assicurare la consistenza dei criteri di sicurezza, soprattutto se applicata in maniera trasparente tra ambienti fisici e ambienti virtualizzati.

La disponibilità di ambienti operativi e applicativi certificati come punti di riferimento (*gold standard*) è in grado di garantire la conformità

e le condizioni operative ottimali effettuando l'identificazione di istanze virtuali non aderenti ai requisiti aziendali: in tal senso, **l'automazione della creazione di istanze virtuali** (*virtual server provisioning*) consente di creare immagini virtuali di riferimento sulle quali applicare piattaforme di base, software applicativo, utenze e regole aderenti a norme amministrative e legali, e di gestirne il ciclo di vita dall'inserimento negli ambienti di produzione all'eventuale ritiro e successiva passivazione.

I temi relativi alla sicurezza virtualizzata richiedono una gestione strutturata e integrata con i **sistemi di gestione delle anomalie** (*incident and problem management*), per un numero di ragioni: minimizzare i fermi macchina e limitare gli impatti causati dai disservizi sugli utenti, tema attuale e particolarmente caldo nel caso dell'erogazione di servizi a un pubblico vasto attraverso il Web o in Cloud.

La commistione tra ambienti fisici e virtuali pone una lente d'ingrandimento su temi già esistenti, come la **gestione dei ruoli** (*role management*), che le aziende hanno già iniziato ad affrontare, e che possono subire una forte accelerazione dall'uso di servizi virtualizzati: le riorganizzazioni aziendali e i cambi di mansione spesso non riflettono tali variazioni sui diritti di accesso a sistemi, applicazioni e dati considerati critici. Una gestione proattiva dei ruoli associati alle identità digitali degli utenti, estesa anche ai sistemi virtuali, può assicurare, in sinergia con tecniche di **prevenzione perdita dati** (*data loss prevention*), un controllo fine

sull'accesso a informazioni pregiate ed eventuali azioni correttive per mantenere la conformità.

SICUREZZA E VIRTUALIZZAZIONE: LA SICUREZZA COME SERVIZIO IT

- Oltre ai temi di unificazione dell'infrastruttura di sicurezza IT per ambienti eterogenei fisico-virtuali, esistono altri *driver* in grado di catalizzare l'attenzione e gli investimenti verso iniziative orientate al business e al generale miglioramento dei servizi offerti ai propri clienti, oltre all'onnipresente Cloud computing, anch'esso in equilibrio tra la promessa di riduzione dei costi e la verifica dell'efficacia in ambienti aziendali. La frontiera dell'innovazione, e forse il "collante" tra gestione della sicurezza e ambienti virtualizzati, è la possibilità di disegnare e realizzare i servizi di sicurezza aziendale attraverso un **catalogo self-service**. Oltre alle caratteristiche innovative e il vantaggio economico derivato dalle componenti di automazione, la fruizione della sicurezza attraverso un catalogo di servizi predeterminati presenta vantaggi tangibili: la capacità di applicare i criteri di sicurezza in maniera preventiva, con un conseguente risparmio, e l'utilizzo di tecniche di contabilizzazione (*metering*) per calcolarne l'uso e i consumi da parte degli utenti interni. L'approntamento di un catalogo self-service della sicurezza rappresenta uno degli obiettivi da centrare per applicare metodi, criteri e best practices *prima* dell'insorgere di eventuali problemi. E, anche nel mondo della sicurezza, prevenire è meglio che curare.