Cloud & Business

n.79
Marzo 2019

LA RIVISTA PER IL MANAGER CHE DEVE OTTIMIZZARE COSTI E PROCESSI

IN QUESTO NUMERO>>>

COVER STORY

I SERVIZI DI ARUBA ENTERPRISE ABILITANO LA DIGITAL TRANSFORMATION DI AZIENDE E PA

di Giuseppe Saccardi

Aruba sviluppa la collaborazione nata con il progetto "Digital Doc", la piattaforma ideata per Decathlon per la digitalizzazione di procedure e processi documentali

Reportec Cloud&Business - Numero 79 - Marzo 2019 - Registrazione al tribunale n°574 del 5 Novembre 2010 -
Tutti i marchi sono di proprietà delle relative società- Editore: Reportec Srl (**www.reportec.it**) - Direttore responsabile: Giuseppe Saccardi
In redazione: Gaetano Di Blasio - Grafica: Paola Saccardi - Immagini: Dreamstime.com

Reportec

Aruba, attiva nei servizi di data center, cloud, web hosting, e-mail, PEC e registrazione domini, è stata scelta da Decathlon, noto marchio francese diffuso in Europa e nel mondo per la produzione e distribuzione di articoli sportivi, per ottimizzare e digitalizzare i propri processi interni nell'ambito di un ampio progetto di Digital Transformation.

Decathlon ha un network internazionale che impiega oltre 80.000 persone in 44 Paesi del mondo ed opera prevalentemente su due aree: da un lato lo studio, la concezione e la produzione di articoli sportivi, dall'altro il retail locale e online di prodotti e servizi.

In Italia Decathlon è presente con 122 punti vendita, 4 siti logistici e 2 uffici di produzione e conta circa 7000 dipendenti.

La collaborazione con Aruba nasce per l'avvio del progetto Digital Doc, una piattaforma di consultazione interna grazie alla quale ogni collaboratore dipendente ha a disposizione tutta la propria documentazione personale, oltre a quella relativa alla contrattualistica del proprio punto vendita e alle policy generali.

Si tratta, ha spiegato Aruba, di un progetto estremamente personalizzato e progettato sulle esigenze dell'azienda, che ha visto l'azione di Aruba Enterprise in tre differenti aree d'intervento:

- sezione sicurezza: è stata realizzata una dashboard tramite cui i direttori possono monitorare costantemente le formazioni della propria equipe e verificare in tempo reale, ad esempio, il flusso di aggiornamento dei corsi di sicurezza ed assicurarsi che tutto sia in regola, secondo quanto previsto per legge;
- sezione azionariato: dedicata ai dipendenti che intendono possedere delle azioni aziendali, comprende la gestione dei flussi di sottoscrizione, cessione e consultazione dell'andamento dei propri investimenti;
- sezione per la gestione del personale: oltre che per gestire le nuove assunzioni, è l'area tramite cui è possibile consultare i cedolini paga e tutti i documenti relativi alla vita lavorativa del collaboratore, quali ad esempio la variazioni della base oraria, sede di lavoro, retribuzione, inquadramento ed ulteriori dettagli.

L'ideazione e la progettazione dell'architettura IT realizzata ex-novo da parte del team di Aruba Enterprise ha previsto anche l'integrazione di determinate soluzioni di Trust Services in questo percorso di Trasformazione Digitale: nello specifico, varie tipologie di firma, quali la Firma Grafometrica, la Firma Digitale Qualificata e la Firma Remota - utilizzate per la dematerializzazione dei documenti durante le fasi di assunzione dei dipendenti nei diversi punti vendita in Italia - e la Conservazione Digitale a Norma di tutti i documenti emessi nelle varie fasi, dai contratti con i dipendenti e

i fornitori, ad eventuale altra documentazione da archiviare.
Queste soluzioni sono parte della gamma di servizi spesso utilizzati dal settore retail che Aruba, in qualità di Certification Authority accreditata, eroga direttamente dai propri Data Center, Rating 4, garantendo massima resilienza e sicurezza a livello di mantenimento dei dati per il business di Decathlon.
L'approccio consulenziale e di stretta collaborazione tra i team tecnici coinvolti ha consentito di centralizzare tutta la documentazione e snellire quei flussi che sono sempre più strategici per un'azienda che, come Decathlon, oltre ad essere dislocata su tutto il territorio, è in continuo ampliamento.

Andrea Sassetti, Aruba

Marco Labianca, Decathlon

In pratica, grazie all'intera infrastruttura IT, Decathlon ora dispone di maggiore sicurezza, ha la possibilità di tracciare tutti i flussi e rendere più agevole la consultazione delle informazioni a tutti i suoi dipendenti, beneficiando inoltre di tempo ed effort economico.
«Siamo orgogliosi di poter collaborare con una importante realtà internazionale come Decathlon mettendo a sua disposizione oltre 10 anni di know-how aziendale sui servizi qualificati e avanzati in ambito di dematerializzazione: in questo modo diamo il nostro contributo - in qualità di interlocutore del mondo IT - alla strategia di business dell'azienda, favorendone la trasformazione digitale, con processi più efficienti e, da non sottovalutare, supporto concreto al tema della sostenibilità ambientale che si potenzia proprio grazie a queste tecnologie», ha commentato **Andrea Sassetti**, Direttore dei Servizi di Certificazione di Aruba.
«Tra le differenti ipotesi identificate, abbiamo apprezzato e ritenuto proficui la proposta e la flessibilità dell'approccio di Aruba, che ha dimostrato di essere un partner disponibile al dialogo e in grado di creare da zero e strutturare processi non preconfezionati, ma tagliati su misura - ha affermato **Marco Labianca**, Procurement Category Manager di Decathlon - Aruba ci ha, letteralmente, accompagnato in questo percorso grazie ad un team Enterprise altamente qualificato e preparato che ci ha ascoltato e, interpretando le nostre esigenze, ha saputo ripensare i nostri processi interni fornendoci delle soluzioni di gestione documentale i cui benefici si stanno estendendo anche ad altri ambiti aziendali».

Qualifica AgID per il cloud alla PA

Aruba è stata qualificata da AgID come Cloud Service Provider (CSP) per erogare servizi Cloud alle Pubbliche Amministrazioni. Nello specifico, è stata qualificata come CSP di tipo C, cioè dotata di un'infrastruttura capace di erogare servizi di livello IaaS, PaaS e SaaS.
La qualifica si inserisce nella fase di digitalizzazione che sta investendo anche la PA italiana: nel contesto della Strategia per la Crescita Digitale del nostro Paese e del Piano Triennale per l'Informatica nella PA, AgID ha infatti previsto un percorso di qualificazione per tutti i soggetti pubblici e privati che intendono fornire servizi cloud alla Pubblica Amministrazione.
Le qualifiche riconosciute da AgID riguardano diversi tipi di soggetti, tra cui fornitori di infrastrutture IT, piattaforme PaaS e software house. Nel caso dei CSP, si assicura che i loro servizi siano sviluppati e operati secondo criteri di affidabilità e sicurezza considerati necessari e idonei per i servizi digitali della PA.

Inizia a trovare spazio, quindi, il concetto di "cloud-first": alla PA è richiesto un primo approccio obbligato ai servizi cloud. L'obiettivo è ottenere un panorama più lineare, in cui la PA utilizzi servizi e infrastrutture cloud che risultino omogenei e i provider forniscano soluzioni cloud in linea con le caratteristiche organizzative, di sicurezza, performance e scalabilità, interoperabilità, portabilità e conformità legislativa del momento.

È a partire dal 1 aprile 2019 che la PA dovrà adottare servizi cloud – IaaS, PaaS e SaaS – che siano esclusivamente qualificati da AgID e pubblicati nel Cloud Marketplace (Catalogo dei servizi Cloud qualificati per la PA); tra questi è disponibile 'Aruba Virtual Private Cloud', un servizio IaaS che permette di acquistare quantità variabili di risorse computazionali, rete e servizi aggiuntivi - come ad esempio il Cloud DRaaS e il Cloud Bare Metal Backup - e attraverso la console web VMware vCloud Director, creare e gestire in completa autonomia i propri data center virtuali, completi di funzionalità evolute come firewall perimetrali, bilanciatori e concentratori VPN, garantendo massima flessibilità e scalabilità.

Gabriele Sposato, Aruba

Il servizio è stato pensato per offrire le massime prestazioni, rete a 10 Gbit/sec, server con processori di ultima generazione, storage ridondato e replicato in modalità sincrona su un data center secondario per garantire il backup e la ridondanza di qualsiasi dato presente.

Grazie alla qualifica ottenuta, Aruba eroga quindi servizi cloud sia alle PA - realtà complesse, generalmente caratterizzate da livelli di delega di competenze e capacità operativa molto diversificate - sia alle Software House che si occupano di SaaS e che, per via dei requisiti richiesti da AgID, devono necessariamente dichiarare su quale infrastruttura sviluppano i propri servizi: in questo senso, il fornitore SaaS può continuare ad avvalersi di un CSP qualificato che abbia quindi già risposto a tutti i requisiti, facilitandosi nei suoi processi di erogazione dei servizi.

«La frammentazione dei sistemi informativi di molte PA rappresenta oggi un ostacolo concreto per l'innovazione. Snellire e migliorare processi e sistemi e sviluppare servizi in modo che siano sempre più adeguati alle esigenze di cittadini e imprese è fondamentale - ha commentato **Gabriele Sposato**, Direttore Marketing di Aruba S.p.A. -. Come Aruba, continuiamo ad essere al fianco della Pubblica Amministrazione e dei partner tecnici specializzati, come le software house, per contribuire concretamente al processo di abilitazione di infrastrutture e servizi in Cloud per la PA. Lo facciamo in modo concreto aiutando i clienti a raggiungere i propri obiettivi e fornendo assistenza nell'intera fase di trasformazione dei sistemi e processi IT. Finalmente oggi ci sono le condizioni giuste perché il processo di Cloud Enablement acceleri anche in ambito PA. Questo porterà benefici per tutti, in primis per cittadini ed imprese».

ACHAB RILASCIA SERVIZI DI GESTIONE CHE ABILITANO L'ASSISTENZA REMOTA CROSS PLATFORM

Controllo remoto multi piattaforma, flessibilità e sicurezza le principali caratteristiche della nuova soluzione ISL Online distribuita da Achab

Achab, società specializzata nella distribuzione di soluzioni software a valore, ha annunciato di aver siglato un accordo con ISL Online per la distribuzione dell'omonima soluzione di remote desktop, che semplifica l'assistenza remota grazie ad un approccio cross platform.
Forte di un'expertise di oltre 15 anni, dal 2003 ISL Online è considerata, ha evidenziato Achab, una delle aziende pioniere nel settore del supporto da remoto. La soluzione ISL Online, in particolare, permette di fornire supporto ai vari dispositivi fissi o mobili, sia PC che Mac o Linux, abilitandone il controllo remoto con un click.
Gli utenti interessati a ricevere supporto possono richiedere una sessione di assistenza tramite la desktop app, il sito web, l'url o la mail di invito.
Gli MSP che utilizzeranno ISL Online hanno anche l'opportunità di fornire ai propri clienti un'assistenza tempestiva e in sicurezza grazie alla connessione criptata tra i device con chiave di cifratura AES 256-Bit, senza dover aprire porte in ingresso sul firewall e senza realizzare una VPN.
«L'obiettivo di fornire una risposta sempre più concreta e aderente alle esigenze degli MSP italiani, ci ha portati a valutare positivamente l'inserimento di ISL Online tra le soluzioni attualmente distribuite da Achab in Italia perché si tratta di un prodotto in grado di offrire un supporto remoto a 360° decisamente più evoluto rispetto ad altre piattaforme già note», ha commentato **Andrea Veca**, CEO di Achab.
Tra i principali vantaggi offerti da ISL Online e evidenziati vi è anche la possibilità di ridurre i costi di gestione grazie alla sottoscrizione di un'unica licenza che permette di installare il software su un numero illimitato di workstation.
In questo modo è possibile fornire supporto remoto ad un numero illimitato di clienti, senza problemi nella creazione degli account operativi che compongono il team di supporto.
Non ultimo, diventa inoltre possibile controllare ed operare anche da smartphone senza pagare una licenza aggiuntiva.
«Sul mercato le soluzioni di remote desktop disponibili sono parecchie, tuttavia riteniamo che offrire un vantaggio competitivo reale significa provvedere all'erogazione di funzionalità e caratteristiche di livello superiore in grado di semplificare notevolmente le procedure di assistenza tecnica. Abbiamo scelto ISL Online per ampliare il ventaglio delle proposte ACHAB perché rispetto ad altre piattaforme offre una maggiore flessibilità grazie alla possibilità di utilizzare il programma su cloud pubblico, privato, on premise o in MPC (Manage Private Cloud)», ha commentato **Claudio Panerai**, CTO di Achab.

PROTEZIONE CONTINUA NEL CLOUD DEGLI UTENTI PRIVILEGIATI CON CYBERARK

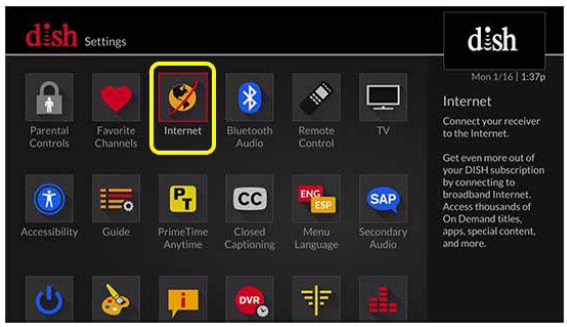
La nuova soluzione di CyberArk per la sicurezza degli accessi privilegiati garantisce la individuazione e la protezione continue dai rischi nel cloud

CyberArk, specializzata in sicurezza degli accessi e degli utenti privilegiati, ha rilasciato nuove funzionalità per semplificare l'individuazione dei rischi e assicurare in ambienti cloud la protezione continua degli account privilegiati.
La "CyberArk Privileged Access Security Solution v10.8" consente l'automazione dell'individuazione dei rischi, l'alert e la risposta ai rischi per account Amazon Web Services (AWS) non gestiti e potenzialmente a rischio.
La versione dispone di nuove funzionalità Just-in-Time che si posizionano al top del settore e che assicurano un accesso flessibile per l'utente ai sistemi Windows, sia basati su cloud sia on-premise. «La gestione del rischio non può limitarsi ad essere solo un processo reattivo. I rischi aziendali di origine digitale possono essere individuati, anticipati, previsti e valutati tramite azioni preventive prioritarie che permettano di modificare la sicurezza dell'organizzazione» suggerisce la società di analisi Gartner.
In pratica, con la nuova release v10.8, CyberArk Privileged Access Security Solution si propone di definire un nuovo standard e di abilitare un approccio esaustivo e al top del settore per quanto concerne la sicurezza e l'efficienza operativa nel cloud attraverso:

- Identificazione continua degli account privilegiati: identifica gli account privilegiati in AWS, come gli utenti IAM (Identity and Access Management) non gestiti, e le istanze e gli account EC2. Le organizzazioni possono in pratica tracciare le credenziali di AWS ovunque siano create e come sono create, e accelerare il processo di on-boarding degli account non gestiti.
- Rilevazione e risposta automatica agli exploit: permette di inviare avvisi prioritari inerenti comportamenti potenzialmente rischiosi, quali ad esempio attività che bypassano il vaulting, il furto della chiave di accesso o una inadeguata gestione. La soluzione CyberArk è anche in grado di assumere il controllo su questi account e attivare una nuova chiave di accesso o una sua rotazione automatica per mitigare il rischio.
- Installazione semplificata in ambienti AWS: estende le funzionalità esistenti per la protezione dell'infrastruttura cloud. Diventa possibile semplificare l'implementazione di CyberArk Privileged Access Security Solution in AWS con AMI per tutti i componenti principali, inclusi il vaulting, la gestione delle sessioni e l'analisi delle minacce.
- Accesso just-in-time con opzioni di provisioning flessibili: permette all'amministratore di configurare la durata concessa per l'accesso ai sistemi Windows, sia che si tratti di cloud o di apparati on-premise. L'obiettivo è di consentire alle organizzazioni di ridurre in modo significativo la problematica operativa per gli end-user e mitigare il rischio costituito da un accesso privilegiato senza restrizioni.

DYNATRACE OTTIMIZZA IL SERVIZIO DI CUSTOMER CARE DI FTD E DISH

Migrato con Dynatrace sul Cloud la piattaforme di eCommerce e l'intero ambiente IT, compreso i microservizi. Il risultato è una customer experience di alto livello



In occasione dell'evento Perform 2019 di Dynatrace, FTD e DISH, organizzazione quest'ultima di reti TV satellitari, hanno illustrato i vantaggi ottenuti in termini di business con l'adozione della piattaforma Dynatrace.

Operando su piattaforme legacy che utilizzava da diversi anni, FTD ha iniziato il suo percorso con Dynatrace per trasformare l'intera piattaforma end-to-end.

«Le nostre piattaforme erano vecchie e la nostra azienda aveva ignorato i progressi tecnologici per un paio di decenni - ha spiegato **Jay Topper**, EVP and Chief Digital Officer FTD Companies. "Così lo scorso gennaio abbiamo deciso di eliminare tutto e ripartire da zero - non si è trattato solo di piattaforme di eCommerce, ma dell'intero ambiente IT. Il 100% è stato creato sul cloud, con Google, portando lì anche tutti i microservizi».

Il passaggio totale su cloud non è stata l'unica mossa compiuta da FTD; la società è passata direttamente all'implementazione di Dynatrace, alcune settimane prima che la nuova piattaforma fosse avviata, lanciandola poi nel loro giorno più impegnativo dell'anno: la Festa della Mamma.

«Non avevamo tempo per imparare a utilizzare il software perché dovevamo essere live. Ma è andata bene così, perché ha funzionato» ha spiegato Topper. DISH ha invece avviato diverse trasformazioni prima di adottare Dynatrace; spostandosi da TV satellitare a cavo, adattandosi alle mutevoli esigenze dei clienti e rendendosi poi conto che era giunto il momento di cambiare i propri sistemi di monitoraggio vecchi di otto anni. Ed è qui che è entrata in gioco Dynatrace.

«Avevamo bisogno di guardare a una nuova soluzione, i nostri sistemi di monitoraggio avevano ormai otto anni - ha spiegato **Eric Wohl**, Senior Vice President of Human Resources -. Quando abbiamo sperimentato un'interruzione di quattro ore durante il nostro POC (purchase order confirmation), l'applicazione che ha riscontrato il problema aveva Dynatrace installato e quando abbiamo dato un'occhiata più da vicino, l'agent di Dynatrace aveva individuato il problema e ci ha detto esattamente quale fosse la causa. Quello è stato il momento in cui abbiamo capito che era la strada giusta da seguire».

«Dynatrace rappresenta lo strumento giusto per noi, e non si tratta solo di un tool operativo, ma di un investimento radicalmente diverso dalla cultura di DISH - ha concluso Eric Whol -. Quando hai i dati di fronte a te e sai che sarai proattivo anziché reattivo e potrai risolvere i problemi prima che accadano, che per noi era in precedenza un compito manuale, questo è un enorme cambiamento e la nostra chiave di svolta».

HITACHI VANTARA RILASCIA SOLUZIONI PER LA CONVERGENZA E LA TRASFORMAZIONE DIGITALE DELLE IMPRESE

Annunciate nuove piattaforme adattative Cisco e Hitachi per l'infrastruttura convergente e un nuovo Partner Program

Hitachi Vantara, azienda interamente controllata di Hitachi, ha rafforzato gli investimenti a sostegno dei propri partner come componente fondamentale per la crescita del business.

Tra le novità annunciate vi sono le nuove soluzioni adattative di Cisco e Hitachi ideate per le infrastrutture convergenti, che rappresentano la dimostrazione pratica delle scelte di Hitachi Vantara in termini di collaborazioni e investimenti in relazioni strategiche.

Con le nuove configurazioni semplificate e ottimizzate Virtual Storage Platform (VSP) per i propri partner e il rinnovato Partner Program, Hitachi Vantara ha in sostanza confermato la sua crescente attenzione verso l'ecosistema dei propri partner, con i quali supportare i propri clienti nell'affrontare le sfide della digital transformation, e creare valore a partire dai dati.

Soluzioni per accelerare la modernizzazione e il cloud dei data center

Un esempio della strategia dell'azienda è offerto da quanto sta facendo con Cisco. Le due aziende stanno valorizzando le rispettive capacità e competenze nella modernizzazione del data center e nel cloud per offrire una soluzione convergente intelligente che aiuti le aziende a superare le sfide di oggi e a competere nel futuro.

Nello specifico, Cisco e Hitachi Adaptive Solutions for Converged Infrastructure è Cisco Validated Design (CVD), una nuova soluzione progettata per soddisfare la domanda di un'infrastruttura convergente, di livello enterprise, in grado di gestire carichi di lavoro delle applicazioni multi-uso e garantire in modo agile ed efficiente la disponibilità continua dei dati e la gestione degli SLA (service-level agreement).

Creati appositamente per la community dei partner, le soluzioni Hitachi VSP PRO, ha osservato l'azienda, consentono di implementare rapidamente e facilmente sistemi di piccole, medie, grandi dimensioni, con un modello di vendita self-service automatizzato che riduce il processo da diverse ore a pochi minuti.

PASSWORD AUTOGESTIBILI DAGLI UTENTI CON GREENLIGHT DI NETCOM

La soluzione, sviluppata da NetCom, permette agli utenti di gestire le proprie password e al service desk di mantenere il processo sotto controllo e di disporre di analitiche

La digital transformation porta numerosi vantaggi ad aziende di ogni settore e dimensione. E' un fenomeno che coinvolge sia il mondo produttivo che i consumatori. Anzi, quest'ultimi, non di rado anticipano per quanto concerne i dispositivi adottati le stesse aziende, essendo meno legati ai processi amministrativi di ammortamento delle infrastrutture IT e più soggetti alle dinamiche del mercato e delle mode.

E' una trasformazione che apporta un forte incremento dei dispositivi fissi o mobili presenti in azienda o presso i consumatori, e se ha il beneficio di migliorare la interazione e la multicanalità nelle realazioni interaziendali e da e verso i clienti, presenta però un rovescio della medaglia che può portare ad un incremento inatteso dell'Opex. Più informatica e più dispositivi in circolazione di crescente complessità, accompagnato da un pari forte incremento di App non sempre di facile utilizzo ed installazione, finisce con l'aggravare il carico di lavoro che devono sopportare gli operatori dediti al supporto di primo o di secondo livello, con l'aumentarne il numero e richiedere maggiori risorse materiali e umane per gestire i ticket originati da un crescente numero di chiamate di supporto. E se non si è in grado di rispondere adeguatamente il rischio è che il cliente is rivolga da un'altra parte.

Il problema della gestione delle password

Ma a questo si aggiunge un altro fattore ancora più critico, soprattutto alla luce del GDPR e normative sulla sicurezza: la gestione delle password dimenticate, smarrite e degli incidenti ad esse relativi che potrebbero inficiare la sicurezza aziendale o aprire contenziosi legali.

Una soluzione a questo critico problema, che potrebbe finire con il creare danni materiali consistenti all'aziendale, al suo brand e al fatturato, l'ha ideata NetCom (netcom.it), una società con sede a Padova costituita vent'anni fa per proporre al mercato soluzioni e servizi di fascia elevata per l'IT Life Cycle Management e l'IT Governance. Annovera oltre 150 clienti nel nord e centro Italia e si caratterizza per una forte presenza in settori che spaziano dalle aziende private (fashion, manufacturing, servizi), alla sanità, la PA locale e centrale, il mondo accademico, il settore finanziario e della grande distribuzione.

«Investiamo molto sulla qualità della consulenza, per tale ragione i nostri consulenti sono certificati sulle best practice più consolidate (ITIL, Prince2, PMI, Microsoft SAM, etc) e sulle principali soluzioni software proposte (EasyVista, Ivanti, Snow, SCCM, etc)» ha osservato **Fabio Mavaracchio**, CEO di NetCom.

GreenLight e la gestione sicura delle password

GreenLight è la soluzione ideata da NetCom con

GreenLigth abilita controlli e analitiche in tempo reale

l'obiettivo di permettere alle aziende di essere compliant con il GDPR e ridurre drasticamente il numero di ticket che gravano sul Service Desk, in modo da contenere in maniera significativa i costi legati alle richieste di assistenza, anche in outsourcing, e di azzerare o quasi i tempi di attesa dell'assistenza tecnica.

Vista dall'utente, è una soluzione per il recupero automatico e in autonomia della password che consente agli utenti stessi di reimpostare le proprie password rispondendo a domande predefinite o inviando un codice di verifica via SMS o e-mail; esattamente come avviene per le APP che utilizzano quotidianamente.

«L'applicazione è fruibile tramite un'interfaccia semplice e chiara, ottenuta attraverso un'accurata progettazione. GreenLight garantisce un'adozione rapida da parte di tutti gli utenti senza lunghe e costose implementazioni e corsi di formazione» ha evidenziato Netcom.

Una gestione in quattro step

Quattro gli step del processo coinvolti nella gestione delle password e delle richieste degli utenti

- Accesso e verifica dell'utente: Il sistema controlla in Active Directory se l'account utente esiste, è abilitato e se è possibile eseguire il ripristino della password. Per aumentare la sicurezza, all'utente può essere richiesto di inserire un codice Captcha.
- Identificazione del chiamante: L'utente deve rispondere correttamente alle domande predefinite o inserire i codici di controllo ricevuti via SMS o email. Solo dopo aver completato con successo questo passaggio l'utente può proseguire.
- Reset della password: GreenLight cambia e/o sblocca automaticamente la password dell'utente in Active Directory.
- Raccolta dei dati: Nel Service Desk viene creata traccia dell'evento, specificando la tipologia di servizio richiesto.

In pratica, non è più necessario, come evidenziato, attendere l'assistenza da parte del Service Desk per gestire le richieste di recupero ed è possibile procedere con la reimpostazione delle password h24 direttamente a partire dalla schermata di accesso di Windows.

GreenLight affronta anche il problema di una identificazione sicura del chiamante. Tre le modalità previste dall'applicazione.

La prima prevede che vengano fornite risposte di carattere personale.

La seconda l'inserimento di un one-time code che viene inviato all'utente via mail.

Una terza modalità prevede in alternativa alla mail l'invio di un one-time code inviato ad un numero di cellulare.

Ogni evento viene poi tracciato nel sistema di Service Desk in modo da disporre di uno storico dettagliato degli interventi attuati, sia che si tratti del comune reset di una password, che della modifica di un profilo o del cambio delle risposte richieste a un utente.

Controlli e analitiche in tempo reale

Oltre a fornire gli strumenti per rapidi e sicuri interventi nella gestione degli eventi interessanti gli utenti, l'applicazione fornisce anche funzionalità atte a razionalizzare l'operatività degli utenti e degli operatori.

Ad esempio, la funzione di "Smart Enrollment" permette di inviare solleciti periodici agli utenti che non hanno completato il processo di iscrizione, quella di "Data Analytics" controlla costantemente l'utilizzo del prodotto e come evolve il trend delle iscrizioni degli utenti, la "Welcome page" illustra al primo contatto di un utente i benefici che può avere e come funziona il prodotto e, non ultimo, la "Common Password Check" effettua la verifica in tempo reale se una password è di tipo comune e può essere facilmente individuata da terzi.

OVH ANNUNCIA SERVIZI KUBERNETES E NUOVI DATA CENTER IN ASIA-PACIFIC

Dopo il rilascio recente di servizi Kubernetes gestiti, OVH annuncia la disponibilità di due nuovi data center cloud che ampliano la sua presenza in Asia e Pacifico

OVH, provider mondiale di cloud hyperscale che ha come mission dichiarata quella di fornire alle aziende impegnate nella trasformazione digitale e nella razionalizzazione di Capex e Opex, valori e prestazioni al top del settore Leader europeo, ha annunciato l'espansione con nuovi servizi di public cloud in estremo oriente e nel Pacifico.

Va osservato che la società, fondato nel 1999 e il cui motto è "Innovation for Freedom", dispone alla data di 28 data center situati in 12 siti in 4 continenti, implementa la propria rete mondiale in fibra ottica e gestisce l'intera catena dell'hosting. Il Public Cloud OVH, ha evidenziato, rappresenta una delle principali soluzioni "Infrastructure as a Service" (IaaS) a livello globale basate su OpenStack oggi esistenti.

Nuovi Data Center Cloud in Asia e Pcifico

In linea con la sua strategia di espansione con nuovi servizi e nuove aree mondiali servite, ha annunciato l'espansione dei servizi di Public Cloud grazie a due nuovi data center attivati nella regione Asia-Pacifico (APAC) e situati a Singapore e a Sydney.

Tramite essi le aziende nella regione APAC possono disporre dell'utilizzo di infrastrutture locali per IaaS caratterizzate da una elevata resilienza e velocità di connessione, nonché di un trasferimento dati più rapido.

Nella vision di OVH l'espansione si prefigge di costituire un valore aggiunto anche per i suoi clienti in Europa, Medio Oriente e Africa (EMEA) che desiderano sviluppare il proprio business su larga scala e che avranno la capacità di distribuire le risorse Public Cloud in APAC, oltre che in tutte le reti esistenti di OVH.

«Con la disponibilità delle soluzioni Public Cloud nell'area Asia-Pacifico, ci impegniamo a sviluppare nuove tecnologie in questa regione e miriamo a supportare la crescita degli utenti cloud locali. Tutto ciò si sposa con la nostra strategia multi-locale, ponendo i data center fisicamente più vicini agli utenti finali. Questo porta vantaggi anche ai nostri clienti EMEA che intendono sviluppare business in APAC, dove OVH opera dal 2016», ha commentato **Michel Paulin**, CEO di OVH.

Tutti i servizi disponibili nelle nuove regioni includeranno anche l'accesso alla rete mondiale di OVH di 16 Tbps e servizi anti-DDoS gratuiti. Sarà inoltre disponibile il servizio vRack, che consente di connettere i servizi di tutto il mondo in modo isolato, e che permette agli utenti di costruire complesse infrastrutture private multi-data cen-

ter.
A livello ingegneristico e architetturale il Public Cloud OVH è basato sul software open source OpenStack e comprende un ampio portfolio di servizi che spaziano ad esempio da istanze CPU/RAM bilanciate (per applicazioni web o aziendali) a elevate prestazioni di elaborazione e ideate per grandi database e big data sino a istanze GPU progettate per applicazioni di intelligenza artificiale.

Kubernetes più semplice con Managed Kubernetes Service

L'annuncio dell'espansione territoriale segue a brevissima distanza quello sulla disponibilità sul proprio Public Cloud dell'offerta Managed Kubernetes Service, progettata allo scopo di per rendere più semplice ai clienti l'utilizzo di Kubernetes all'interno della sua infrastruttura e permettere loro di concentrarsi sul proprio core business sgravandoli dai problemi associati alla manutenzione del software e dell'infrastruttura.
L'offerta di Managed Kubernetes Service include:

- Load Balancer, integrato nativamente con Kubernetes
- Aggiornamento delle policy di sicurezza a cura del cliente
- Scelta tra le versioni 1.11 e 1.12 di Kubernetes, le ultime due versioni fornite dalle varie offerte di servizi gestiti disponibili sul mercato.

La proposta di Kubernetes comprende la fornitura di uno standard comune tra i provider di servizi cloud ibridi e multi-cloud. Come uno dei peraltro non molti fornitori certificati CNCF in Europa, OVH ha anche deciso di implementare un'alternativa Kubernetes alle offerte esistenti, in modo da garantire libertà di scelta, reversibilità e trasparenza per gli utenti.

LE AREE GRIGIE DELL'IT E COME AFFRONTARLE

L'IT aziendale presenta aree critiche e per affrontarle serve la conoscenza. Il come è approfondito da Marco Rottigni, Chief Technical Security Officer di Qualys

La visibilità è una vera sfida oggi, a causa della situazione confusa che la Digital Transformation porta con sé. Questo, osserva **Marco Rottigni**, Chief Technical Security Officer EMEA di Qualys, perché i confini dell'IT aziendale si espandono con l'adozione del cloud, il numero degli endpoint aumenta con l'enterprise mobility e il ciclo di vita dello sviluppo software (SDLC) si estende con i DevOps.
Non è l'unica sfida, ma la visibilità resta indubbiamente lo step fondamentale per tutti i processi volti ad armonizzare l'IT, predisponendo sicurezza e conformità necessarie all'interno di ogni realtà aziendale.
La risposta risiede nel comprendere ma per

Marco Rottigni, Qualys

farlo, osserva Rottigni, servono "occhi": sensori che potenziano la raccolta dei dati e che sono studiati appositamente per gli ambienti di elaborazione in cui vengono implementati.
Successivamente, questi dati vengono normalizzati per facilitarne la visibilità e, arricchiti con un contesto appropriato fatto di dati non rilevabili, per alimentarne la comprensione e la capacità aziendale di gestione delle risorse.
Per quanto concerne i servizi on-premise dell'ambiente IT moderno, la visibilità riguarda server, client, dispositivi di rete, dispositivi di sicurezza ed altri tipi di host, su piattaforme di più sistemi operativi. Peraltro, la virtualizzazione, che è oggi standard de facto nei data center, include agilità e flessibilità di istanziare server e client molto rapidamente.
Infine, la situazione è aggravata dai dispositivi IoT connessi a reti cablate e wireless, che hanno scarse possibilità di essere installati con qualsiasi software o agente. Come è allora possibile avere la piena certezza di non essere vulnerabili? Come si può esser sicuri che il nuovo software adottato dall'azienda sia incluso nella golden image?
La situazione è di certo complessa ma rimanendo sempre nella sezione on-premise dell'ambiente IT, andrebbero considerati, mette in guardia il manager, altri due fattori che contribuiscono ad aumentare la complessità: il primo è l'Enterprise Mobility, il secondo è la containerizzazione.
Con Enterprise Mobility si fa riferimento a quegli utenti che, per viaggiare o lavorare da remoto, escono dal perimetro aziendale, e recentemente questo bisogno di mobilità è incrementato grazie a dispositivi performanti come tablet, chioschi e sistemi computerizzati sempre più leggeri. Ciò comporta ulteriori criticità in termini di visibilità: come garantire che i dati siano elaborati in modo sicuro? Come fare a verificare che questi dispositivi non vengano utilizzati per ottenere accesso indesiderato alla rete e ai dati?
La containerizzazione rappresenta da parte sua un nuovo modo di supportare l'ambiente IT, un metodo rivoluzionario per velocizzare l'implementazione dell'infrastruttura: introduce agilità, grande flessibilità e potenza … ma non agevola la visibilità, osserva Rottigni, e non è difficile essere d'accordo con lui..
Oltre alle preoccupazioni che riguardano lo scenario on premise, sempre in termini di visibilità, negli ambienti IT moderni si aggiungono altri due elementi critici: l'adozione del cloud e i DevOps.
E' pur vero che il cloud, spesso, comporta il disassemblaggio dell'infrastruttura tradizionale in parti più piccole: archiviazione, logica applicativa, funzioni, rete, logica di bilanciamento del carico, database, gestione di identità, di accesso e altro ancora.
Questo implica la creazione di relazioni tra queste parti, ma, ci si può legittimamente chiedere, dove e quando sono state implementate queste parti e come si gestisce la loro sicurezza?
La soluzione a tutte queste sfide può basarsi, spiega Quali, solo su un approccio strategico ed olistico che permetta di concentrarsi su aspetti quali:

- La visibilità su tutto il panorama IT.
- L'accuratezza nel normalizzare i dati durante lo screening.
- La scalabilità verso l'alto e verso il basso.
- L'immediatezza nel raggiungimento dei risultati.
- La consapevolezza dello stato dell'arte.

Queste cinque capacità, nella vision di Qualys, dovrebbero essere implementate o rafforzate da un punto di vista strategico, fondate su strumenti e tecniche per supportare le procedure basilari.
Un approccio pragmatico potrebbe focalizzarsi sull'analisi accurata del panorama IT che si possiede, cercando di comprendere i vari e differenti ambienti di cui si compone, e sulla relazione tra questi: ad esempio, se gli ambienti di produzione si espandono al cloud, o se il cloud viene utilizzato principalmente per lo sviluppo e area di con-

trollo qualità.
«Per aiutare ad affrontare questi problemi abbiamo sviluppato una piattaforma olistica, evolvendo l'approccio di disaccoppiamento della raccolta dei dati, realizzato con sensori specializzati distribuiti in tutto il panorama IT, dall'elaborazione dei dati, eseguiti centralmente all'interno della nostra piattaforma cloud. Questo approccio offre la coerenza necessaria per visualizzare, riepilogare, approfondire e aggregare i dati per più profili utente; questo approccio fornisce la consapevolezza della situazione a supporto del processo decisionale e dei processi come SecOps» ha spiegato Rottigni.

AL VIA EVA, LA CYBERSECURITY TARGATA STORMSHIELD

La nuova linea di soluzioni per la sicurezza IT virtualizzate supporta i reparti IT incaricati di ottimizzare i costi operativi del cloud attraverso una gestione appropriata delle risorse

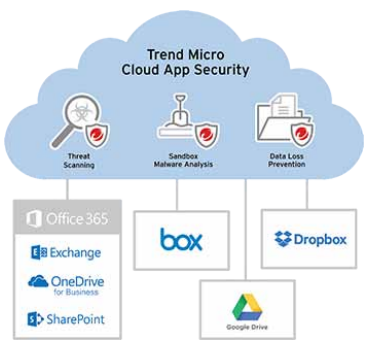

Marco Genovese, Stormshield

Con la nuova gamma di firewall UTM/IPS modulari e ad alte prestazioni SN2100, SN3100 e SN6100 per la tutela proattiva delle reti aziendali annunciati lo scorso ottobre, Stormshield ha posto il suo primo tassello di una strategia di più ampio respiro, attraverso cui il produttore europeo di soluzioni per la cybersecurity si propone di fornire alle aziende clienti tecnologie atte a favorire una sicurezza evolutiva e un più rapido ritorno sull'investimento.
Conformemente a questa strategia, Stormshield ha annunciato la disponibilità di EVA (Elastic Virtual Appliance), una nuova a linea di soluzioni per la sicurezza delle aziende che affrontano il percorso della virtualizzazione della propria infrastruttura IT come estensione o in sostituzione alle infrastrutture tradizionali.
«Trasformando i costi d'acquisto in costi operativi, l'inarrestabile migrazione su piattaforme cloud private o pubbliche di servizi altrimenti fruibili attraverso infrastrutture classiche, comporta sia un cambiamento di paradigma nell'allocazione dei budget IT, sia modifiche in termini di contabilizzazione dei canoni, dovute alla variazione della modalità di fatturazione dei servizi», ha spiegato **Marco Genovese**, Product Manager Stormshield Network Security.
Le proposte degli operatori cloud sono sempre più spesso elastiche, ovvero basate sulle risorse e sulla potenza di calcolo effettivamente utilizzate. «Si tratta di formule che rappresentano una nuova sfida per i reparti IT, a cui viene demandata l'ottimizzazione dei costi operativi

attraverso una gestione più appropriata delle risorse, come la CPU dei sistemi virtualizzati, la RAM o lo spazio di archiviazione» ha aggiunto Genovese.
Le soluzioni Stormshield Elastic Virtual Appliance sono state sviluppate appositamente per consentire di modificare rapidamente e in maniera semplice le risorse allocate al sistema in base alle esigenze del momento, adeguando il consumo delle risorse nel cloud alle effettive necessità. Lato prestazioni e potenza, le soluzioni Stormshield Elastic Virtual Appliance si adeguano automaticamente alle capacità di vRAM e vCPU allocate dall'hypervisor.
L'adattamento automatico alle risorse dedicate a EVA ne semplifica ulteriormente il roll-out, permette di integrare la soluzione facilmente nel corso dell'implementazione di nuovo servizio virtualizzato, e le conferisce la necessaria flessibilità per adattarsi ai futuri sviluppi dell'infrastruttura cloud aziendale.
La varietà di ambienti virtualizzati supportati (Citrix, VMware, KVM and Hyper-V), ha commentato l'azienda, assicura al reparto IT la massima libertà di scelta dell'infrastruttura, la possibilità di variare facilmente la piattaforma cloud impiegata ove necessario (Amazon Web Services o Microsoft Azure) e di migrare la propria soluzione di cybersecurity in concomitanza con la migrazione di altri servizi.

CLOUD APP SECURITY HA BLOCCATO 9 MILIONI DI MINACCE A OFFICE 365

Trend Micro ha rilasciato il report Cloud App Security 2018, dedicato alla soluzione che costituisce un secondo livello di protezione per Office 365



Trend Micro, tra i leader nella cybersecurity, ha comunicato che nel 2018 la sua soluzione Cloud App Security ha rilevato e bloccato quasi 9 milioni di minacce ad alto rischio indirizzate a Office 365.
Nel dettaglio, Cloud App Security ha bloccato 1 milione di malware (1.080.022), quasi 8 milioni di attacchi di phishing (7.736.815) e 100mila tentativi di truffe Business Email Compromise (103.955).
L'anno scorso le minacce bloccate dalla soluzione erano state solo, si fa per dire, 3,4 milioni.
I dati sono inconfutabili e rivelano come la continua crescita delle minacce via email esponga le organizzazioni a rischi sempre maggiori di subire frodi, attività di spionaggio e furto di informazioni, sottolineando l'importanza di investire in una protezione multilivello quando si utilizzano piattaforme online, come Office 365.
Le email sono in tutto il mondo uno strumento

efficace di comunicazione e collaborazione e i cybercriminali continueranno a colpire questa piattaforma, cercando di mettere a segno i loro attacchi.

«Le organizzazioni adottano sempre più servizi email in cloud, per migliorare la produttività e l'agilità, ma il report di Cloud App Security rivela come sia fondamentale adottare un secondo livello di protezione per difendersi dagli attacchi di phishing o Business Email Compromise» ha commentato **Kevin Simzer**, chief operating officer at Trend Micro.

Cloud App Security è una soluzione di Trend Micro che protegge Microsoft Office 365 Exchange Online, OneDrive for Business e le piattaforme online SharePoint.

Agisce come un secondo livello di protezione dopo che le email e i file sono stati scansionati dalla sicurezza interna di Office 365.

L'obiettivo di Cloud App Security è di contrastare la proliferazione delle minacce email, utilizzando il machine learning e le analisi sandbox per malware, ransomware e altre minacce avanzate.

La soluzione ha recentemente aggiunto anche nuove capacità che combinano tecnologie di intelligenza artificiale e computer vision per individuare finti siti web.

Questa tecnologia è applicata anche per identificare le email di phishing dopo che sono stati implementati filtri relativi al mittente, al contenuto e alla reputazione URL.

Va infine osservato che Trend Micro utilizza l'intelligenza artificiale anche per la soluzione Writing Style DNA, che individua specificatamente gli attacchi Business Email Compromise.