

Persone & Conoscenze

La voce della Direzione del Personale

Luglio/Agosto/Settembre 2022

L'HR tra le nuvole

Proteggere e gestire i dati
del personale nel cloud



Elsa Marasca
con la collaborazione
di **Monica Giambersio**

Il mercato del software HR è dominato da due tipologie di sistemi: quelli nati e utilizzati on premise (cioè in locale) e quelli adattati al cloud successivamente. Descritti come web-based, cloud-based, forniti online o come Software as a service (SaaS), queste soluzioni condividono diverse caratteristiche, per esempio il fatto che il software è ospitato dai fornitori in un ambiente 'esterno' all'azienda, accessibile online. Nonostante, offrono la comodità di uno strumento sempre aggiornato (spesso senza costi extra). Questo scenario sta facendo emergere diverse questioni, come la gestione della sicurezza dei dati del personale. Come garantire l'attenzione riguardo a questo aspetto? Ne abbiamo discusso con esperti e player del settore.

1. Riccardo Barone, Responsabile della Pres vendita delle Soluzioni Cloud per il Mondo HR Italia & Iberia di Oracle
2. Giovanni Basilico, Account Executive di Personio
3. Fabio Cardilli, Product Manager HCM di **Talenti** Software
4. Luba Manolova, Direttrice della Divisione Microsoft 365
5. Nicola Uva, Growth Marketing Senior Director di ADP

Con il nuovo *mindset* digitale, conseguenza più evidente della ripresa post pandemica, il settore dell'HR Tech (cioè le soluzioni digitali dedicate al mondo delle Risorse Umane) sta acquisendo una posizione centrale per la crescita delle imprese. A confermarlo sono i numeri: a livello mondiale, questo mercato valeva 53,1 miliardi di euro nel 2021 e ha previsioni di crescita fino a 90 miliardi nel 2025 (in Europa, lo scorso anno c'è stato un giro di business da 7 miliardi di euro).

A delineare lo scenario è l'analisi *Il mercato HR Tech & i nuovi trend del settore* che Cross Border Growth Capital, advisor per aumenti di capitale e operazioni di finanza straordinaria per startup e Piccole e medie imprese (PMI), ha realizzato in collaborazione con Cosmico, Recruiting & Learning Platform italiana. Nel frattempo, però, aumentano anche gli attacchi *ransomware* e *malware* (cioè virus che prendono il controllo del computer di un utente ed eseguono la crittografia dei dati, per poi ripristinare il normale funzionamento del dispositivo solo dopo il pagamento di un riscatto). Secondo l'ultimo report della società globale di cybersecurity Trend Micro, l'Italia ha attualmente il triste primato in Europa per attacchi di questo tipo e si mantiene nelle prime 10 posizioni dei Paesi più bersagliati anche a livello globale. Dall'analisi, risulta che i cinque mercati più colpiti dai cybercriminali in Italia sono stati: Pubblica amministrazione (Pa), Sanità, Tech, Manifatturiero e Banking. A maggio 2022, il 58,6% delle minacce è arrivato via email. In questo contesto, è

possibile per la funzione HR proteggersi adeguatamente per tutelare tutti i dati sensibili che gestiscono attraverso soluzioni in cloud?

Salvaguardare i dati con l'Intelligenza Artificiale

Per Riccardo Barone, Responsabile della Prevendita delle Soluzioni Cloud per il Mondo HR Italia & Iberia di Oracle, la risposta va in una direzione precisa, visto che, sul tema della sicurezza dei dati, la multinazionale del settore informatico ha compiuto una scelta strategica: controllare tutti gli asset tecnologici del servizio cloud che propone al mercato, dall'hardware al livello applicativo, senza il coinvolgimento di terze parti. Barone sottolinea la scelta di investire circa 6 miliardi di euro l'anno nelle piattaforme cloud per favorire efficienza e sicurezza. "Adottiamo policy interne al di sopra dei livelli internazionali, ci scambiamo informazioni criptate e nessuno dei nostri dipendenti ha accesso ai dati in chiaro dei clienti, se non è autorizzato", precisa il manager.

Il colosso informatico ha da poco aperto in Italia una Cloud region –che utilizza un Data center locale– attraverso la quale sono erogati i servizi cloud, ma ne ha realizzate altre in Francia e Spagna, puntando su sicurezza e sovranità sul dato, nel rispetto delle normative e delle regolamentazioni di ogni Paese. A ciò si aggiunge il fatto che il cloud di seconda generazione di Oracle si avvale di un approccio "security by design", secondo il quale la protezione dei dati è considerata sin dalla progettazione: il tutto è, infatti, presidiato da Intelligenza Artificiale (AI) e Machine learning (ML), che permettono di evitare accessi non consentiti e migliorare autonomamente le performance in base alle informazioni utilizzate. "Abbiamo messo AI e ML,

Foto di Saep ICT

Spin8, la suite proprietaria sviluppata per il commercio online





L'Italia ha attualmente il triste primato in Europa per attacchi informatici e si mantiene nelle prime 10 posizioni dei Paesi più bersagliati anche a livello globale

che fanno parte nativamente dei nostri sistemi, al servizio del controllo degli accessi. Così i nostri clienti ricevono costantemente alert e suggerimenti, in base a una serie di policy legate al ruolo organizzativo delle persone che accedono alle informazioni”, racconta Barone. Sul fronte dell'utilizzo dei software, non sono richieste competenze particolari. Per il manager la facilità d'uso deve, infatti, essere garantita non solo all'HR, ma anche a responsabili di linea e collaboratori, che devono poter avere accesso ai servizi digitali con la stessa comodità con cui fanno un acquisto online o un post sui social media. “In questo senso, l'azienda investe molto sulla *user experience*. La caratteristica che contraddistingue l'offerta dei diversi prodotti è la soluzione *mobile responsive*”, specifica Barone. Puntando su questa modalità di fruizione, il risultato è che il cliente sceglie quali servizi erogare dai dispositivi mobili, come smartphone e tablet, e l'accesso per gli utenti è semplice come inquadrare un QRCode.

La sicurezza dei dati passa da soluzioni mirate e su vari livelli

Quando si parla di sicurezza, spesso si pensa al backup dei dati, ai firewall, agli antivirus. Invece, la sicurezza si realizza su tre livelli: l'applicativo software, il Data center in cui è ospitato e le modalità di accesso all'applicativo da parte degli utenti HR e degli stessi dipendenti. Tutti questi elementi concorrono al livello di sicurezza dei dati all'interno dei software in cloud di ADP, multinazionale specializzata nelle soluzioni per la gestione delle Risorse Umane. Lo spiega Nicola Uva, Growth Marketing Senior Director di ADP, che traccia un quadro delle strategie adottate dall'azienda nell'ambito della sicurezza informatica. “In ADP si investe in ognuno di questi livelli utilizzando i principi internazionali per la cybersecurity. Quando si dice che la sicurezza parte dalla progettazione del software, bisogna verificare che il database in cui i dati sono memorizzati sia realizzato in modo tale da rendere complessa l'associazione di dati sensibili con il loro proprietario; per esempio, quelli retributivi o relativi a visite mediche vanno memorizzati in modo che risulti molto difficile collegarli alla persona a cui appartengono (attraverso tabelle separate)”, sottolinea Uva. Un discorso analogo è fatto per la gestione delle password, per le quali si adottano criteri stringenti legati alla lunghezza delle parole, al tempo di validità o al numero massimo di tentativi di accesso.

Il secondo livello si riferisce al Data center che ospita l'applicativo. ADP ha scelto Data center di livello quattro, ovvero ridondati a livello geografico: il principale in Francia e una sua copia esatta in Spagna. “In questo modo,

qualsiasi problema possa capitare non si bloccano processi critici, quali il calcolo e il pagamento degli stipendi dei dipendenti”, spiega Uva.

Il terzo livello riguarda le modalità di accesso agli applicativi; si tratta forse del più importante di tutti per l'esperto, perché è quello più sottovalutato. “ADP ha adottato misure estremamente stringenti che vanno dai Pc, notebook e cellulari aziendali, tutti criptati con cancellazione automatica in caso di furto, all'impossibilità di accedere a siti pericolosi ai filtri sulla posta elettronica, per evitare errori nello scambio di documenti sensibili e molto altro”, continua Uva.

Quindi, nella scelta di una soluzione cloud che gestisca i processi del Personale e contenga i dati sensibili delle persone, per Uva occorre fare una valutazione completa dei tre livelli; ma questo non è sufficiente se non si formano gli utenti e i dipendenti, al fine di adottare processi e comportamenti virtuosi. Riguardo al futuro di queste soluzioni, Uva sostiene che la parola d'ordine sarà “flessibilità”, abbinata agli investimenti di medio e lungo termine. “Il sistema cloud può essere arricchito con l'acquisto di soluzioni verticali e specifiche, utilizzabili nella forma *pay for use*, anche per un periodo di tempo limitato e per problematiche ben determinate, come nel caso delle App per smartphone”.

Puntare sul cloud per proteggere i dati

Per Fabio Cardilli, Product Manager HCM di Talenti Software, fornitore di soluzioni HR e Finance per aziende di medie dimensioni, il SaaS non è sinonimo di scarsa sicurezza del dato; al contrario, rispetta una serie di leggi stringenti tra cui il regolamento europeo su privacy e dati, General data protection regulation (Gdpr): “In questi software HR sono presenti anche i *vulnerability assessment*, ovvero analisi costanti (per esempio annuali) per identificare le potenziali vulnerabilità di sistemi e applicazioni e valutare il danno di un eventuale attacco hacker”. Tali strumenti fanno parte di clausole contrattuali da parte di società terze. Gestire, invece, la propria sicurezza in autonomia per le aziende è molto più costoso. “Si tratta di un ambito molto legato alle versioni dei software, che nel cloud sono costantemente aggiornate, anche dal punto di vista della cybersecurity. Nelle soluzioni *in house*, gestite internamente dall'azienda cliente, gli *upgrade* sono a carico della propria struttura IT”, spiega Cardilli. Un'altra garanzia che alcuni vendor forniscono, tra cui Talenti Software, è la certificazione ISO 27001 per i sistemi informativi, cioè la norma internazionale che definisce i requisiti per impostare un



I cinque mercati più colpiti dai cybercriminali in Italia sono stati: Pubblica amministrazione, Sanità, Tech, Manifatturiero e Banking

sistema di gestione della sicurezza delle informazioni aziendali, con lo scopo di proteggerle. “Forniamo funzionalità a supporto del rispetto della normativa, garantendo, per esempio, l’esercizio del diritto all’oblio per le persone che lasciano l’azienda o la portabilità dei dati nel caso in cui si cambino fornitori. Il pacchetto di soluzioni si paga con una sottoscrizione annuale e il vantaggio riguarda l’assenza di costi legati all’hosting della soluzione”, precisa Cardilli.

In generale, secondo il Product Manager di **Talentia** Software, la caratteristica che una soluzione SaaS deve avere, in accordo con i nuovi trend, è di essere il più possibile *codeless*, ovvero senza necessità di personalizzazioni attraverso la gestione delle righe di codice di programmazione. “La natura di questi software ora si basa sulla configurazione dei sistemi e non sulla struttura *custom* del prodotto, come in passato. La configurazione è più adattabile ai diversi bisogni e compatibile al requisito di aggiornamento continuo”, sottolinea Cardilli. La sfida, secondo l’osservatorio di **Talentia** Software, è trovare il giusto trade off tra queste due esigenze, cioè la necessità di personalizzare le soluzioni e il requisito *codeless*. Oggi sono richieste, infatti, piattaforme *user oriented*, agili e vicine all’esperienza mobile. Da qui, il cambio di ruolo dell’IT: “Questa funzione non interviene più nell’ambito dell’implementazione delle soluzioni, ma nell’integrazione tra software HR e altre applicazioni per le Risorse Umane, come i sistemi di autenticazione o quelli per la gestione delle paghe”, conclude Cardilli.

Ripensare il modo di lavorare attraverso la tecnologia

La sicurezza delle informazioni è un punto cardine cui le aziende devono prestare la massima attenzione anche secondo **Luba Manolova, Direttrice della Divisione Microsoft 365**, dedicata all’omonima soluzione dell’azienda informatica, che integra le tecnologie di

Office 365, Windows 11, Enterprise Mobility Suite, security e compliance: “Applichiamo criteri di sicurezza specifici nel mondo IT che permettono di configurare la protezione e la prevenzione della perdita di dati sensibili”. Le soluzioni di cybersecurity e compliance di Microsoft sono integrate *by design* nei prodotti e servizi e hanno lo scopo di proteggere end-to-end i *digital estate* dei clienti, ovvero le risorse e le infrastrutture IT necessarie per supportare i processi e le operazioni aziendali, e i dati, cioè il *data estate* delle organizzazioni. “La nostra tecnologia aiuta nel gestire la protezione di informazioni confidenziali e sensibili con accessi condizionali. Non si può mai, per esempio, aprire l’allegato di un’email se chi lo invia non ne autorizza l’accesso. Inoltre, le informazioni sensibili sono crittografate a monte e protette se scambiate via chat, email o conservate nei documenti”, chiarisce Manolova. Un altro elemento su cui si è puntato è l’offerta di sistemi che non richiedano agli utenti finali competenze specifiche, tramite la configurazione guidata dei software e con una serie di policy che si possono personalizzare in base alle necessità dei diversi settori aziendali. “Il trend che si vuole favorire è l’accrecimento di competenze digitali nell’HR per guidare le persone in un contesto più tecnologico rispetto al passato, grazie all’AI e all’automazione dei processi”, spiega Manolova. L’idea proposta è, quindi, di sfruttare la tecnologia come punto di partenza per ripensare il modo di lavorare, ponendo al centro le persone con una collaborazione sempre più importante tra HR e IT e le altre funzioni aziendali, per rispondere al meglio alle esigenze della forza lavoro. Microsoft ha lanciato una nuova piattaforma di *employee experience*, direttamente integrata nell’hub di comunicazione e collaborazione utilizzato giornalmente

dalle persone, che favorisce la creazione di dinamiche di gruppo. Inoltre, con l’AI si può tenere sotto controllo il rischio di sovraccarico lavorativo e stanchezza digitale, per favorire la ricerca del benessere attraverso l’equilibrio tra vita privata e lavorativa. “In ottica di semplificazione dell’esperienza, è possibile accedere direttamente dalla piattaforma di comunicazione e collaborazione al modulo di Intranet aziendale, dove si possono consultare news, comunicazioni importanti dell’azienda e interagire nelle community d’interesse, oppure favorire l’apprendimento continuo integrando nel flusso di lavoro i corsi di formazione, ricercando informazioni utili su determinati temi o tra i colleghi e chi sta lavorando sugli stessi”, conclude la manager.

Il futuro è nell’automatizzazione dei processi

Giovanni Basilico, Account Executive di Personio, società di software nata in Germania e operativa in tutta Europa, specializzata nella gestione delle Risorse Umane, racconta che nella sua azienda sono state implementate e sono in continuo sviluppo misure di sicurezza tecniche e organizzative, basate sulle indicazioni del documento Gdpr europeo, su standard e linee guida comuni, come

Adottare soluzioni mobile con consapevolezza

Utilizzare un'App per prenotare scrivanie, sale riunioni e parcheggio per molte persone è sempre più frequente, soprattutto per chi deve lavorare in ambienti ibridi in cui si alterna la presenza in ufficio con quella da remoto. Ora, a portata di smartphone arrivano anche cartellino e busta paga, un'ulteriore comodità accolta positivamente. Lo dimostra la recente ricerca di F2A (azienda italiana specializzata nell'erogazione di servizi HR, anche in modalità SaaS), che, a partire da una piattaforma online, ha sviluppato una soluzione mobile per la gestione e l'amministrazione del personale. Attraverso l'analisi dei dati -aggregati e anonimizzati- dei circa 200mila utenti totali del software (desktop e mobile), è emerso che il documento più visualizzato è il cedolino. Particolarmente gradito è anche il servizio di compilazione del cartellino, strumento utilizzato da un utente su tre. È, infine, riconosciuta come indispensabile l'archiviazione digitale dei documenti, come per esempio attestati di formazione, Cud o regolamenti aziendali. Tale funzione, seppur facoltativa, è, infatti, scelta dal 100% delle società clienti: "Tra i principali utilizzatori dell'App spiccano i più giovani (sette 20enni su 10), ma anche le generazioni più adulte sembrano valutare positivamente la novità tecnologica. Emerge, così, l'identikit di un lavoratore sempre più *smart* che, abituato all'onnipresenza delle tecnologie *mobile* nella quotidianità e nel tempo libero, adotta volentieri la digitalizzazione anche nella propria sfera lavorativa", dichiara **Giorgio Colagrossi, Direttore R&D di F2A**.



Giorgio Colagrossi,
Direttore R&D
di F2A

Una protezione a più livelli

L'obiettivo aziendale è fornire ai clienti un servizio sicuro, che risponda alle esigenze HR e liberi i CIO dalle innumerevoli preoccupazioni legate alle questioni di privacy e cybersecurity. In quest'ottica, le infrastrutture di produzione F2A sono situate presso outsourcer esterni, certificati con le normative ISO 27001, ISO 20000 (primo standard internazionale, sviluppato specificatamente per la gestione dei servizi IT) e ISO 45001 (norma internazionale che specifica i requisiti per un sistema di gestione della salute e sicurezza sul lavoro). Esse sono, inoltre, protette da vari livelli di firewall (componente di difesa della Rete) in alta affidabilità, con sistemi automatici di prevenzione e meccanismi di AI. "Le applicazioni, invece, sono progettate in maniera sicura fin dall'inizio, con controlli di sicurezza standard e solidi, per monitorare il ciclo di vita di sviluppo del software sicuro", spiega Colagrossi. Fondamentale, infine, per il Direttore R&D di F2A, è una continua formazione: "Solo nel 2021 sono state svolte 1.270 ore di formazione sulla cybersecurity, coinvolgendo 635 dipendenti".

ISO 27001, e sui principi base della protezione IT divulgati dall'Ufficio Federale tedesco per la sicurezza informatica (Bsi). I dati dei clienti, inoltre, rimangono in Europa. "Gli aspetti innovativi di una piattaforma in cloud sono la possibilità di essere sempre aggiornata e la sua velocità di attivazione: nel nostro caso ci vogliono dalle quattro alle sei settimane, e molto raramente è necessario il coinvolgimento del reparto IT", spiega Basilico. Appena firmato il contratto, il team di implementazione di Personio si mette in contatto con l'ufficio HR per l'avvio della soluzione. Attualmente, il software si può integrare con più di 100 piattaforme e App, come LinkedIn, Slack e Google Calendar.

La vision della società è che la tecnologia per HR renda automatici i processi manuali, che richiedono l'impiego di tempo e risorse e spesso fanno incorrere le persone in errori a causa della ripetitività dell'azione da svolgere. "Ci piacerebbe che la funzione Risorse Umane si occupasse delle persone, senza caricarsi di compiti amministrativi, che potrebbero essere facilmente automatizzati", specifica il manager. In questo modo, è più semplice focalizzarsi sugli elementi strategici del proprio ruolo.

"Faccio un esempio: quando viene assunta una nuova persona, con pochi clic il team HR può attivare un processo automatico che informa tutta l'organizzazione dell'inizio dell'*onboarding* della risorsa e, allo stesso tempo, dà al neoassunto accesso a materiali utili per il suo inserimento", racconta Basilico. All'interno di un'organizzazione consapevole della necessità di gestire il rischio, quindi, al di là degli strumenti tecnologici che sono predisposti a salvaguardare i dati, è opportuno che il dipartimento HR svolga un ruolo attivo e centrale nel preservare e proteggere la sicurezza dell'azienda. Lo può fare formandosi e formando tutti i dipendenti sui protocolli, con argomenti che vanno dalla sicurezza della posta elettronica all'accesso e all'utilizzo di dati riservati, al riconoscimento di minacce e attività dannose, diffondendo una cultura della responsabilità nell'applicare le procedure e le politiche di sicurezza.

FINE