Customer Management insights

GDPR e fake data, come superare le sfide legate a privacy e sicurezza

L'evoluzione tecnologica rende sempre più sofisticate anche le minacce al nuovo petrolio dell'economia digitale, i dati dei clienti. La sfida numero uno per le aziende è ora quella di trovare nuove soluzioni per tutelare utenti e business.

Emma Pisati
CMI Customer Management Insights

C'è una data che si avvicina e che è probabilmente cerchiata in rosso nelle agende di tutte le aziende europee o operanti in Europa: è il 25 maggio 2018, giorno in cui entrerà in vigore il GDPR (General Data Protection Regulation), la nuova normativa sulla privacy per l'UE, a detta di alcuni la più profonda ridefinizione delle norme relative alla data protection dalla nascita della Rete. Sono rimasti poco meno di cento giorni per adeguarsi alle novità introdotte, ma pare che le idee di numerose aziende siano ancora piuttosto confuse in proposito, e la strada da percorrere per garantire una maggiore sicurezza e un maggior controllo in materia di gestione dei dati personali appare tutt'altro che spianata davanti a loro.

GDPR, questo sconosciuto: quali novità per privacy e sicurezza

La data menzionata è in realtà l'ultima tappa di un percorso iniziato nel 2016, anno di nascita ufficiale del Regolamento GDPR UE 2016/679, documento che stabilisce rigorosi requisiti globali per la tutela della privacy, regolando le modalità di trattamento e protezione dei dati personali in modo che siano maggiormente rispettate le scelte e i diritti delle persone fisiche cui questi fanno riferimento, valido per aziende di ogni tipo e dimensione.

LE DOMANDE

Si tratta di un riconoscimento a livello giuridico e normativo della centralità assunta dai dati – e dalla loro protezione – nell'economia e nella società digitale, alla cui base possono essere individuati sei principi fondamentali:

- trasparenza nell'uso e nella gestione dei dati personali;
- limitazione dell'utilizzo per scopi specifici legittimi;
- limitazioni precise per la raccolta e l'archiviazione;
- maggior controllo sui dati personali riconosciuto ai singoli individui cui tali dati si riferiscono;
- archiviazione dei dati per il solo tempo necessario allo scopo che ne ha motivato la raccolta;
- protezione adeguata dei dati attraverso pratiche di sicurezza appropriate.

A conferma dell'aria di cambiamento che si respira ormai nel mercato europeo in materia di sicurezza e data protection possiamo citare l'esempio di Facebook, che a inizio anno ha rafforzato la privacy garantita ai suoi utenti realizzando un nuovo e unico centro privacy a livello globale, garantendo agli utenti una gestione dei dati più semplice e prevedendo inoltre di raddoppiare a 20.000 il numero degli addetti al controllo sicurezza.

Stop a vulnerabilità e confusione nelle aziende

A livello teorico sembra tutto chiaro, ma nella pratica le difficoltà sono ancora molte.

Secondo un recente studio di Accenture, l'Italia è tra i primi 10 Paesi al mondo maggiormente colpiti da crimini informatici (che interessano soprattutto le aziende dei settori finance ed energia), con un aumento dei costi del cybercrime rispetto al 2016 pari al 23%.

Dalla privacy by design alla valutazione d'impatto, passando per l'istituzione di nuove figure aziendali come il responsabile della protezione dei dati, sono numerose le indicazioni fornite dall'UE alle aziende affinché possano adeguare le loro strategie e tecnologie per la sicurezza alle nuove sfide e alle nuove minacce che caratterizzano il panorama digitale, ma soprattutto affinché si diffonda e venga interiorizzata una vera e propria cultura della privacy e della sicurezza, riconosciuta come il mezzo più efficace per vedere effettivamente riconosciuti i diritti e i doveri sanciti dalle nuove regole.

Fake data: l'autodifesa dei clienti

Le aziende hanno quindi molto lavoro da fare, tra attacchi che si moltiplicano – e che diventano sempre più sofisticati con l'utilizzo di IoT e intelligenza artificiale – e normative più stringenti, ma anche i clienti sembrano non rendere loro la vita facile.

Al crescere della loro consapevolezza in merito alle minacce e agli attacchi mirati a ciò che di più prezioso è oggi presente sul mercato – i loro dati e informazioni personali – gli utenti sono ormai pronti a tutto pur di metterli al sicuro da ogni possibilità di violazione. Tra le iniziative in tal senso recentemente rilevate da una ricerca di RSA, la nuova tendenza è quella di fornire *fake data* per evitare di condividere informazioni personali con le aziende.

È facile intuire che se il 30% dei clienti in Italia fornisce false informazioni alle aziende, questo non può non avere un impatto negativo sul business.

Ma i consumatori italiani non si fermano qui: il 64% degli intervistati ha dichiarato che la reputazione aziendale in materia di gestione dei dati dei clienti influenza le loro scelte d'acquisto, il 56% sostiene che eviterà di fornire i propri dati a un'azienda che in passato si è "macchiata" della vendita o dell'utilizzo degli stessi senza consenso, mentre il 64% afferma di essere pronto a boicottare completamente quelle organizzazioni che hanno ripetutamente mostrato di non trattare con la dovuta attenzione il tema della protezione dei dati. Ma ogni medaglia ha il suo rovescio, e questa non fa eccezione: le aziende che si dimostreranno effettivamente in grado di gestire in modo responsabile e di proteggere i dati incontreranno il favore e la fiducia del 58% degli italiani che hanno già dichiarato di essere pronti e ben disposti ad acquistare i loro prodotti e servizi.

CMI - CUSTOMER MANAGEMENT INSIGHTS
Anno 7 - N. 1 - Febbraio 2018
Numero unico

Direttore responsabile: Letizia Olivari
letizia.olivari@cmimagazine.it

Redazione: Emma Pisati
redazione@cmimagazine.it

Impaginazione e grafica: Matteo Olivari
grafica@matteoolivari.it

Sito web: L'Ippocastano
art@lippocastano.it

Abbonamenti on line:
www.cmimagazine.it/abbonamenti

Informazioni commerciali:
tel. +39 02 87259135
commerciale@cmimagazine.it

CMI Customer Management Insights
è una testata specializzata realizzata da
L'Ippocastano Srl
P. Iva 03328430966
via Valparaiso, 8 - 20144 Milano

Per garantire sicurezza e privacy occorre che clienti e aziende imparino a maneggiare al meglio i dispositivi e i dati oggi a disposizione: quali sono i livelli attuali di consapevolezza e attenzione nella gestione e condivisione dei dati?

Carolina Losa
Responsabile Marketing Basisgroup

La sicurezza informatica e la tutela di privacy e dati sono snodi imprescindibili nei processi di digital transformation. Faccio un esempio: quante volte durante la giornata ci capita di dover inserire o modificare le nostre password per accedere ai servizi online? Cambiare o creare nuove password può essere un'operazione noiosa, ma è una delle tante operazioni quotidiane necessarie, perché i rischi sono sempre dietro l'angolo. Per evitare realmente questi rischi, i livelli su cui bisogna operare in termini di protezione sono dati, dispositivi e identità. Ma parliamo del livello di consapevolezza di tutto questo. Secondo una ricerca del 2016, l'87% dei manager ha ammesso di aver caricato dati e informazioni aziendali sui propri account personali. Questo vuol dire che il rischio è duplice, poiché non si limita più ad account e device aziendali. "Ci sono due tipi di grandi aziende, quelle che sono state violate e quelle che non sanno di essere state violate" ha affermato James Comey, Direttore FBI: per evitare questo è necessario non limitare la protezione dei dati ad azioni di riparazione, ma renderla un'attività costante, preventiva e culturale.

Valentina Trevaini
Direttore Commerciale LiveHelp

Le aziende sono già molto sensibili su questo argomento, tant'è che in questi ultimi mesi c'è stato molto fermento fra i nostri clienti. Sicuramente il livello di reattività alle nuove normative dipende dal settore, poiché alcune realtà trattano con più frequenza i dati sensibili dei propri utenti e si tratta di normative in continua evoluzione. Le imprese che già seguono le disposizioni della legge 196/2003 ora dovranno aggiornare l'informativa sulla privacy, dando più evidenza alle finalità e ai mezzi della raccolta dati, e probabilmente anche avvalersi di un DPO. È proprio la nascita di questa nuova figura a essere fondamentale, perché dovrà verificare la situazione aziendale e assicurarsi che il titolare del trattamento dati segua le procedure indicate nel nuovo GDPR. Per questo motivo ci stiamo accreditando come DPO: vogliamo dare la migliore consulenza ai nostri clienti per arrivare preparati al 25 maggio, data ultima per l'adeguamento alla nuova legge europea.

Piergiorgio De Campo
Co-founder, Direttore Generale e Cto Noovle

L'ultima ricerca su questi temi – condotta da Trend Micro e Opinium su un campione di 1.132 decisori IT di aziende con più di 500 dipendenti e appartenenti a 11 Paesi – rivela che, nonostante una robusta conoscenza legata ai temi del GDPR, il livello di consapevolezza e attenzione di manager e responsabili aziendali è ancora molto eterogeneo. Per esempio, se il 79% dei business leader è convinto che i propri dati siano protetti al meglio, il 64% del campione dichiara di non essere a conoscenza che la data di nascita di un cliente è classificata come dato personale. Inoltre, il 42% non farebbe rientrare i database di e-mail fra i dati sensibili, il 32% non lo farebbe con gli indirizzi di domicilio e il 21% con l'indirizzo e-mail personale. In aggiunta la ricerca rivela che gli intervistati non sono sicuri di chi debba essere identificato come responsabile in caso di perdita di dati EU da parte di un service provider USA. Solo il 14% identifica correttamente la perdita di dati come una responsabilità di entrambe le parti. C'è anche confusione su chi debba essere responsabile nell'assicurare la conformità con il GDPR. Per il 31% la responsabilità è del CEO, mentre per il 27% è del CISO e del team security. È chiaro quindi che le aziende hanno ancora molto lavoro da fare per mettere in sicurezza i dati di cui dispongono e per non incorrere nei procedimenti sanzionatori.

Chris Strammiello
Vice President of Global Alliances & Strategic Marketing Nuance Communications

È indubbiamente aumentata la consapevolezza in merito al tema della condivisione dei dati grazie anche a norme e regolamentazioni di conformità. Nel corso degli anni, la maggior parte delle aziende ha rispettato le proprie responsabilità in materia di sicurezza, introducendo le opportune politiche e procedure di protezione dei dati. Tuttavia, con l'inizio dell'anno si è sicuramente rinnovato l'interesse per ciò che le aziende devono fare per essere conformi al regolamento generale sulla protezione dei dati (GDPR).

Alessandro Vallega
GDPR Business Development EMEA Security Oracle

L'introduzione prevista a maggio 2018 del GDPR sta sicuramente incidendo sul modo in cui le aziende devono gestire e usare i dati, soprattutto quelli dei consumatori, e sta alzando il livello di consapevolezza e attenzione, ma c'è ancora molta strada da fare. Gartner a fine 2016 aveva previsto che il 50% delle aziende mancherà in modo significativo questa scadenza, e molti nostri clienti ci stanno confermando questa situazione. Ci sono diversi aspetti da considerare, e per ognuno di essi il livello di maturità "medio" è differente. Mi riferisco all'adeguamento delle informative, alla gestione strutturata del consenso (integrata nel sistema informatico e con la granularità richiesta), alla redazione di un registro dei trattamenti che contemporaneamente sia a norma di legge e colleghi gli asset informativi (data store e applicazioni) ai trattamenti stessi (che è l'unico modo di produrre informazioni adoperabili per il miglioramento dell'IT), alla modifica delle applicazioni per la gestione dei "diritti dell'interessato" (accesso, rettifica, oblio, portabilità, ecc.) e, ultimo ma non meno importante, alla sicurezza del trattamento che richiede di garantire confidenzialità, integrità e disponibilità dei dati in maniera tale da non produrre danni ai diritti e alla libertà degli interessati.

Donato Maraggia
MFP Product Manager Ricoh Italia

Purtroppo nelle aziende c'è ancora una scarsa consapevolezza relativa alla sicurezza delle informazioni, un tema che viene spesso approcciato in modo frammentato, esponendosi così a rischi di notevole entità. Secondo uno studio condotto dal Ponemon Institute nel 2017, il valore totale medio di una violazione ai dati aziendali è stato di 3,62 milioni di dollari. Tale cifra è destinata ad aumentare nei prossimi anni in conseguenza delle normative che, come il GDPR (General Data Protection Regulation), impongono multe alle aziende che non sono in grado di dimostrare la sicurezza delle informazioni, che deve invece diventare una priorità.

Mauro Corvino
Business Development Director, EMEA Center of Excellence SAP Hybris

Le informazioni sulla clientela sono risorse strategiche per le aziende, rappresentano il vantaggio sulla concorrenza e alimentano l'eccellenza operativa. Le strategie aziendali maggiormente legate a iniziative di trasformazione digitale, di innovazione o di impatto sul mondo social richiedono livelli di attenzione maggiori nella gestione e condivisione dei dati. In un mondo digitale iperconnesso, la sicurezza del dato è un fattore imprescindibile, e le informazioni sulla clientela sono la più importante valuta del business. Il regolamento Europeo GDPR 2016/679 nasce per difendere i diritti e le libertà fondamentali dei cittadini europei in relazione ai loro dati personali, intervenendo direttamente nel rapporto innovazione digitale – diritti e libertà delle persone. Alcune aziende, a pochi mesi dall'entrata in vigore del regolamento GDPR, devono ancora intraprendere in modo appropriato il percorso di adeguamento richiesto. C'è ancora incertezza nel capire quali dati siano ritenuti sensibili e chi ne debba essere responsabile all'interno delle organizzazioni. Sono da ritenere necessarie verifiche di sicurezza sui processi di gestione dei dati, sulle procedure di trasparenza e sulla conformità dei sistemi applicativi e delle infrastrutture aziendali.

Rosa Maria Molteni
Marketing and Communication Manager Spitch Italy Srl

La percezione generale e "culturale" di una gestione corretta della privacy è molto alta, sia da parte degli utenti finali che delle aziende nei confronti dei propri clienti. Potremmo dire quasi che ogni prodotto/servizio o soluzione tecnologica offerta debba obbligatoriamente utilizzare la tutela della sicurezza e della privacy come parte integrante e integrata, e non solo per una questione di osservanza legale, ma in qualità di leva per la creazione di valore nella costruzione dell'esperienza del cliente. Attenzione altissima e consapevolezza in crescita da parte di tutti: ogni minima stonatura nella gestione dei dati del cliente viene amplificata e sanzionata in maniera pesante dal mercato esterno, dai competitor e dai consumatori.

Mancano pochi mesi all'entrata in vigore del nuovo GDPR: quali saranno in concreto i cambiamenti che questo comporterà per i clienti?

Carolina Losa
Responsabile Marketing Basisgroup

La data del 25 maggio 2018 è il cambiamento più importante degli ultimi vent'anni in tema di riservatezza delle informazioni e privacy. Per prima cosa è necessario che le imprese effettuino una revisione completa dei dati che raccolgono e trattano, e che individuino le finalità di utilizzo in modo da poter adeguare modalità di trattamento e informativa. Tutte le attività volte all'adeguamento al GDPR, con le relative modifiche che ne conseguono, non sono legate solo al rapporto con l'esterno, ma riguardano anche la struttura interna dell'azienda. Per questo il GDPR istituisce la figura del Data Protection Officer, che ha il compito di vigilare sui processi interni alla struttura aziendale.

Valentina Trevaini
Direttore Commerciale LiveHelp

Grazie al nuovo GDPR, i clienti finali avranno più potere nella gestione dei loro dati personali e/o sensibili, per cui potranno agire direttamente sulle aziende al fine di proteggere la propria privacy: avranno infatti gli strumenti giusti per poter chiedere all'azienda come e perché i dati vengono trattati ed eventualmente modificare, cancellare e avanzare il diritto di oblio degli stessi. In sostanza ci sarà un nuovo livello di consapevolezza e di gestione corretta della privacy. La cosa più importante è che le imprese aggiornino i propri siti web e i propri software, avviando anche un processo di formazione all'interno dell'azienda; il nostro team sta quindi lavorando per formare e informare le aziende e renderle GDPR compliant.

Piergiorgio De Campo
Co-founder, Direttore Generale e Cto Noovle

Come noto, gli obiettivi del nuovo regolamento non vanno solo nella direzione di armonizzare le normative sulla protezione dei dati in tutta Europa, ma intendono restituire ai cittadini UE il pieno controllo sui loro dati, ribadendo alcuni principi già presenti nella vecchia normativa, quali il diritto di rettifica, il diritto di cancellazione (e il diritto all'oblio) e il diritto di limitazione del trattamento. Uno dei fondamentali diritti del cliente – garantito dall'art. 15 del GDPR – è il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un utilizzo di dati personali che lo riguardano e, in caso di risposta affermativa, l'accesso ai dati e a determinate informazioni. L'art. 20 del GDPR, inoltre, introduce il diritto alla portabilità dei dati, secondo cui l'interessato ha la prerogativa di ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano, e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti. Inoltre, nell'esercitare la propria facoltà rispetto alla portabilità dei dati, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati da un titolare del trattamento all'altro, se tecnicamente fattibile.

Chris Strammiello
Vice President of Global Alliances & Strategic Marketing Nuance Communications

Di base il GDPR vuole garantire una maggiore sicurezza, consente di dimostrare di aver messo in atto le misure necessarie per impedire che si verifichi una violazione, nonché di disporre di strumenti di accertamento in grado di individuare l'origine di una violazione qualora si verificasse. Dal punto di vista del flusso di lavoro di stampa e documentale, molte aziende che dispongono di una soluzione di gestione della stampa intelligente o di un'applicazione di stampa protetta sono già ben posizionate per il GDPR. Questo perché tali soluzioni forniscono informazioni dettagliate su chi ha stampato, copiato o scansionato un documento, mentre la stampa protetta impedisce che i documenti finiscano in mani sbagliate.

Alessandro Vallega
GDPR Business Development EMEA Security Oracle

La scadenza del GDPR porta le aziende a focalizzare l'attenzione sul tema del trattamento dei dati come cose preziose, da proteggere a tutti i costi. I dati vanno protetti quale che sia la loro fonte: un dispositivo mobile (che, per inciso, produce anche dati di contesto come la geolocalizzazione), un sensore IoT nel capo di abbigliamento o nella bicicletta da corsa, fino al sistema contabile e amministrativo chiuso negli uffici della sede centrale. Da un punto di vista tecnologico ci si sposterà dalle misure "ovvie" (encryption, anonimizzazione, ecc.) alla gestione delle identità di utenti e oggetti, integrata ed estesa ai sistemi di gestione dei log. Essa gioca un ruolo centrale e strategico per i temi di controllo accessi, di prevenzione degli incidenti e analisi forense ex-post.
La protezione dei dati è la vera sfida da affrontare, e l'attuale offerta Security di Oracle diventa il supporto alla creazione di un sistema di difesa in profondità a più livelli, integrando la multicanalità e la trasformazione digitale – dove il cloud è ormai la tecnologia primaria. La compenetrazione tra azienda fisica e digitale sta trasformando la struttura stessa delle organizzazioni, e per questo è fondamentale garantirne la totale sicurezza.

Donato Maraggia
MFP Product Manager Ricoh Italia

La sicurezza informatica deve estendersi a tutte le tecnologie utilizzate dai clienti. Alla luce del GDPR, è necessario cambiare il modo di gestire i dati innovando le tecnologie e i dispositivi con soluzioni allo stato dell'arte, in grado per esempio di limitare il controllo degli accessi da parte degli utenti o di crittografare i dati memorizzati. Oltre che sulle tecnologie, è opportuno soffermarsi sulle procedure di sicurezza e – aspetto non indifferente – sul coinvolgimento dei dipendenti e sulla loro sensibilizzazione. Un progetto qualificato per adeguarsi al GDPR deve quindi prevedere attività di formazione in modo che tutti abbiano chiara l'importanza della protezione dei dati, non compromettano – anche involontariamente – la sicurezza delle informazioni e sappiano utilizzare in modo corretto tutte le funzionalità di security delle tecnologie.

Mauro Corvino
Business Development Director, EMEA Center of Excellence SAP Hybris

Le nuove normative in materia di sicurezza e data privacy modificano in concreto lo stato dei diritti e doveri stabiliti tra clienti e organizzazioni. In questo contesto di cambiamento giuridico e culturale, sempre più clienti stanno ponendo maggiore attenzione nel comprendere in che modo e perché le organizzazioni usano i loro dati personali. Una recente indagine effettuata nel 2017 da Gigya (società leader nel settore del Customer Identity Access Management) ha rivelato che il 68% dei consumatori negli Stati Uniti e nel Regno Unito ritiene che la gestione dei propri dati personali da parte dei brand non sia corretta. Il primo passo per ricostruire la fiducia dei clienti è fornire loro il controllo e l'accesso trasparente ai dati. Sulla base della sopracitata indagine, il 69% dei consumatori è preoccupato per i potenziali rischi di tutela della privacy dovuti al sempre maggiore utilizzo dei device IoT. Malgrado ciò, il 70% degli intervistati dichiara di utilizzare meno di sette password per i propri molteplici account online, dimostrando una bassa attenzione in materia di "protezione digitale". L'applicazione del regolamento GDPR rappresenta l'entrata in una nuova era in cui i clienti chiedono rispetto per la loro privacy e si aspettano comunicazioni pertinenti e personalizzate quando accettano di condividere informazioni personali. L'attenzione sarà rivolta non solo ai dati personali di tipo "personally identifiable information" (e.g. nome, indirizzo, data di nascita, carta di credito, ecc.) ma anche alle informazioni che consentono di identificare indirettamente l'identità di un consumatore (tracciamento di cookies, post sui social media, indirizzi IP, ecc.).

Rosa Maria Molteni
Marketing and Communication Manager Spitch Italy Srl

Il traguardo di ogni azienda che abbia a cuore la Customer Experience dovrebbe essere quello di agire in modo che i clienti non si accorgano quasi degli ulteriori oneri burocratici per garantire la loro privacy e sicurezza. Il cliente deve sentire che la propria tutela era già completa prima, e quindi sta alle aziende utilizzare eventuali moduli o richieste di dati ulteriori come uno strumento di garanzia aggiuntiva. Le soluzioni tecnologiche che agevolano questi passaggi saranno mirate a semplificare l'iter di compliance, e a creare nello stesso tempo modalità interattive che rispondano a una semplificazione di processi e costi per azienda e cliente.

Quali sono gli aspetti di maggiore vulnerabilità e criticità per la sicurezza e la privacy dei clienti ai quali le aziende devono prestare attenzione?

Carolina Losa
Responsabile Marketing Basisgroup

I rischi per la sicurezza e l'integrità di dati e privacy sono intrinsecamente altamente dinamici, e si evolvono insieme alle tecnologie e alle regolamentazioni. Come tutti i rischi aziendali, questi non possono essere eliminati, ma c'è bisogno di un insieme di azioni coordinate per la loro gestione. Per iniziare ad approcciare questo problema c'è bisogno di definire un terreno aziendale comune, un framework, dove diversi settori aziendali possano riconoscersi e allineare le loro pratiche di cyber security in un processo di evoluzione continua. Ogni organizzazione deve allineare le proprie pratiche di cyber security basandosi sul proprio business, la propria tolleranza al rischio e le risorse che è in grado di mobilitare. Le macro-aree del processo d'implementazione del cyber security framework sono struttura organizzativa, cultura aziendale, programmi di security awareness e cyber security governance.

Valentina Trevaini
Direttore Commerciale LiveHelp

Sicuramente i software antivirus e firewall forniscono aiuto, ma prima di partire dalla sicurezza degli applicativi e dall'analisi dei sistemi di intrusione ci deve essere consapevolezza e formazione in tutta l'azienda, dal singolo impiegato sino al responsabile IT. Grazie a una corretta formazione, la gestione dei dati sarà sicuramente adeguata. È molto importante rendere partecipe tutto il team di lavoro, ed è per questo che la nostra azienda ha programmato momenti di formazione per tutti i dipendenti. A dimostrazione di questo fatto investiremo in formazione, inserendo nel nostro team un DPO accreditato da un ente certificato.

Piergiorgio De Campo
Co-founder, Direttore Generale e Cto Noovle

L'ultimo rapporto Verizon "Data Breach Investigations Report 2017" indica che nel 2016 sono stati violati oltre 4 miliardi di record appartenenti a database aziendali, riguardanti soprattutto dati personali e credenziali di accesso. È auspicabile che l'aumento delle minacce contribuisca ad accelerare i percorsi di compliance, ma quel che è certo è che solo un numero ristretto di aziende ha la possibilità di acquistare soluzioni così avanzate da azzerare in maniera quasi completa il rischio derivante da qualsiasi tipologia di attacco, come evidenziato dall'ultimo rapporto Clusit 2017, che ha tra l'altro identificato il 2016 come l'anno peggiore per la sicurezza informatica – anno in cui, per la prima volta, l'Italia si trova nella top ten degli attacchi più gravi registrati.
Considerata la quantità di dati personali che secondo il nuovo regolamento europeo andrà disciplinata e gestita, occorrerà prestare particolare attenzione nel far sì che tutte le informazioni riportate nei diversi opt-in siano chiare ed esaustive (all'interno di app, portali ed e-commerce); che tutti i dati di opt-in relativi al consenso utente siano gestiti centralmente e allineino in real time tutti i sistemi terzi che sfruttano quel dato (es. i sistemi di e-mail marketing); che le sezioni "my account" dei diversi portali forniscano una serie di possibilità all'utente, tra cui visualizzare in qualsiasi momento le proprie informazioni, modificarle, cancellare il proprio profilo, congelare i propri dati, scaricarli in diversi formati; che vengano eliminati dal database (dopo 36 mesi) gli utenti inattivi, e che sia infine richiesto un sistema di gestione dei metadati.

Chris Strammiello
Vice President of Global Alliances & Strategic Marketing Nuance Communications

È necessario che le aziende utilizzino strategie di protezione dei dati complete e multidimensionali come parte dei loro programmi di prevenzione della perdita di dati. Le aziende investono costantemente per proteggere le loro reti da intrusioni esterne e da ransomware. La realtà è che le violazioni dei dati non provengono sempre da intrusioni esterne, ma in molti casi sono causate da un uso interno improprio di informazioni riservate. Per quanto riguarda la stampa, le aziende devono garantire che le informazioni personali protette non trapelino – sia che si tratti di un formato cartaceo sia elettronico – e che siano visualizzate solo da chi è autorizzato.

Alessandro Vallega
GDPR Business Development EMEA Security Oracle

La complessità degli attacchi automatizzati e il numero di variabili rende impossibile per un essere umano rilevare le minacce in tempo utile. Oracle ha dunque potenziato le suite di sicurezza Oracle Identity SOC (Security Operation Center) e Oracle Management Cloud, servizi cloud per la governance delle identità, il controllo accessi, il monitoraggio dei log e delle configurazioni in (e da) ambienti cloud ibridi che, integrando elementi di intelligenza artificiale, permettono di rilevare automaticamente i comportamenti anomali da parte di utenti o entità connesse in rete e apportare rimedi automatici, riducendo nettamente il rischio e le finestre di esposizione. Per evitare le pesanti sanzioni e altre conseguenze, le aziende sono tenute ad adeguare i sistemi e le applicazioni alla normativa, e Oracle ha già definito un percorso di approccio al GDPR grazie al quale i clienti sono supportati da un apposito framework di soluzioni che è stato messo a punto con l'esperienza maturata sul campo.

Donato Maraggia
MFP Product Manager Ricoh Italia

Ricoh ha individuato quattro aspetti per la sicurezza del digital workplace. Il primo è la capacità di eseguire controlli efficienti dei dati, fondamentale per garantirne confidenzialità e integrità. Il secondo è la conservazione dei documenti che devono essere disponibili per gli utenti senza che ne venga compromessa la sicurezza. Il terzo è la possibilità di rimuovere definitivamente tutti i dati dai dispositivi alla fine del loro ciclo di vita, poiché i dispositivi dismessi rappresentano un rischio per le informazioni aziendali ancora spesso trascurato. Il quarto, infine, è la garanzia di un supporto alle aziende che rafforzi ulteriormente la sicurezza dei dati e mantenga una visione globale di tutti i possibili rischi attraverso consulenza, fornitura e configurazione dei sistemi IT, monitoraggio remoto e assistenza tecnica.

Mauro Corvino
Business Development Director, EMEA Center of Excellence SAP Hybris

Le aziende sono tenute a essere conformi al nuovo regolamento UE e contemporaneamente devono perseguire i loro obiettivi di business. La conformità al regolamento GDPR non è una condizione che, una volta raggiunta, è acquisita per sempre: richiede infatti una continua e attenta gestione nel tempo. Per i manager e i responsabili aziendali l'impatto maggiore che l'entrata in vigore del GDPR avrà è relativo soprattutto alle potenziali sanzioni che eventuali inadempienze potrebbero causare. Danni che dal punto di vista economico potrebbero arrivare a cifre importanti, fino a 20 milioni di euro o al 4% del fatturato globale annuo. Il mancato rispetto del regolamento, inoltre, potrebbe comportare per le aziende una maggiore vulnerabilità dovuta alle continue cyber minacce che sfruttano le inadeguatezze dei sistemi di protezione dei dati per il recupero delle informazioni sensibili. L'entrata in vigore del GDPR porta con sé elementi di semplificazione ma anche ulteriori oneri: per questo motivo molte aziende stanno introducendo all'interno dell'organizzazione nuovi ruoli aziendali connessi alla protezione dei dati personali, quali il Data Controller, il Data Processor e il Data Protection Officer (DPO).

Rosa Maria Molteni
Marketing and Communication Manager Spitch Italy Srl

Spesso le aziende, soprattutto conglomerati risultanti da acquisizioni e fusioni a livello transnazionale, non hanno un'amministrazione unitaria dei sistemi di gestione del cliente o livelli qualitativi e di ottemperanza legale omogenei. Differenze fra Paesi o business unit dovrebbero essere monitorate e preventivamente sanate internamente all'azienda, in vista dei cambiamenti legislativi, segnatamente per quanto riguarda la sede di custodia dei dati e la tutela legale del cliente finale. In particolare, i dati sensibili andrebbero trattati in modalità totalmente ottemperante e restrittiva, senza cedere a scelte di compromesso economico che rischierebbero di avere costi altissimi in termini di perdita di clienti e immagine. Una policy di trasparenza aziendale sulle modalità di trattamento, e persino chiare indicazioni sulle possibilità di recesso, potrebbero essere leve ulteriori per rassicurare il cliente finale.

Quali livelli di sicurezza e privacy riescono effettivamente a garantire le nuove soluzioni per l'identificazione dell'utente o per la fruizione in self-service dei servizi?

Carolina Losa
Responsabile Marketing Basisgroup

Questo è un tema molto caro a Basis Information Technology. Quando parliamo di access management ci riferiamo a un processo in grado di fornire agli utenti i diritti che permettono loro di usare un servizio o un gruppo di servizi ed eseguire le policy e le azioni definite nel processo di information security management. Dotarsi di un sistema di gestione dei processi legati alla creazione, registrazione e gestione delle identità degli utenti – e dei relativi permessi e autorizzazioni – automatizza l'applicazione delle policy di sicurezza e risk

management aziendali. Un sistema corretto impedisce l'implementazione delle richieste di accesso inappropriate, e riduce così i rischi per la sicurezza dell'intero sistema informativo aziendale derivanti da minacce interne ed esterne.

Valentina Trevaini
Direttore Commerciale LiveHelp

Ci sono più livelli di sicurezza, a seconda del dato personale trattato e del contesto in cui viene rilevato. Fermo restando che anche solo il primo livello di sicurezza deve essere garantito, tutto dipende dalla finalità con cui vengono raccolti i dati: è proprio su questo che si basa la nuova normativa. È molto importante che l'azienda decida cosa fare con i dati e che lo comunichi al suo cliente, evitando di raccogliere indirizzi e-mail e nominativi senza uno scopo preciso; ogni campagna marketing deve essere preceduta dalla scelta di un obiettivo. La precisione delle informative varierà poi in base alla finalità del trattamento dei dati. Finalmente questa legge coinvolge concretamente i grossi player (come Google e Aruba) e a cascata chi collabora con loro, per renderli responsabili.

Piergiorgio De Campo
Co-founder, Direttore Generale e Cto Noovle

I nuovi modelli di business, dettati da un'era dominata da un profondo processo di trasformazione digitale, richiedono un'elevata capacità nel saper cogliere, interpretare e tradurre i bisogni specifici dei singoli utenti per poter personalizzare il più possibile i servizi, e garantire allo stesso tempo elevati standard di privacy e sicurezza. Saranno utili strumenti in grado di misurare il livello di GDPR compliance e di suggerire alle aziende indicazioni e azioni correttive da compiere a livello sia organizzativo che tecnologico. Le soluzioni dovrebbero inoltre prevedere la scelta di uno strumento centralizzato e ottimizzato per la gestione dell'identità dell'utente che, da una parte, aiuti le aziende a essere compliant rispetto al nuovo regolamento e a gestire in modo sicuro e strutturato le identità dei clienti e, dall'altra, fornisca agli utenti una Customer Experience ottimizzata e piacevole, per favorirne la fidelizzazione.

Alessandro Vallega
GDPR Business Development EMEA Security Oracle

Un'attenta vigilanza è parte integrante delle migliori pratiche di compliance e security. L'automazione qui può avere un ruolo significativo nell'aiutare a identificare comportamenti anomali e implementare misure di difesa sulla base di criteri prestabiliti. I sistemi devono essere in grado di comprendere in modo intelligente chi sta accedendo alle informazioni, quando e perché, e basare la risposta alla minaccia su modelli creati in precedenza – per esempio chiudere un utente fuori dal sistema prima che possa accedervi, permettere o negare l'uso di dati sensibili e così via. L'immagine del tecnico di un security operations center che fissa i monitor in attesa di riscontrare un allarme è cosa del passato. La risposta ad attacchi automatizzati deve essere fornita da macchine basate su intelligenza artificiale e machine learning. L'uomo osserva e presidia il processo, e indaga (in maniera semplificata) i segnali "deboli" che possono essere indice di un attacco molto più sofisticato. Intelligenza artificiale e machine learning sono gli ambiti dove Oracle si sta distinguendo in modo particolare, e che hanno portato l'azienda a proporre soluzioni all'avanguardia, scalabili e affidabili. Oracle ha aumentato la sicurezza del cloud espandendo i servizi CASB (Cloud Access Security Broker) per offrire visibilità sull'intero stack cloud e uno strumento di automazione della sicurezza. Oracle ha recentemente annunciato anche il primo database autonomo al 100% e le nuove applicazioni automatizzate di cyber security che rilevano e risolvono gli attacchi in tempo reale; si tratta di un database del tutto automatizzato grazie al machine learning, che di fatto elimina la necessità di interventi esterni per la sua gestione ed è accoppiato a un livello di cyber security automatizzata.

Donato Maraggia
MFP Product Manager Ricoh Italia

Uno dei massimi rischi per la sicurezza deriva dal fatto che le persone in azienda godono di accesso illimitato alle aree di lavoro e ai dispositivi. Se non si attuano le opportune misure di sicurezza, i sistemi multifunzione possono essere utilizzati in modo improprio per la diffusione o la copia non autorizzata di informazioni sensibili. È possibile fare in modo che, per poter utilizzare le funzionalità di un multifunzione, un utente debba autenticarsi mediante badge o password. Prendiamo come esempio il printing: quando si utilizza la

funzione "stampa riservata", all'utente che ha effettuato la stampa è associata una password. Il documento viene rilasciato dal multifunzione solo dopo che l'utente si è recato al dispositivo e si è autenticato con badge oppure ha digitato la password sul pannello operativo; questo evita che le pagine rimangano nei vassoi e possano essere lette da persone non autorizzate.

Mauro Corvino
Business Development Director, EMEA Center of Excellence SAP Hybris

Negli ultimi anni la maggior parte delle iniziative di marketing online si sono basate sulla gestione di contatti anonimi, tracciamenti di cookies e third-party data. La normativa GDPR rende necessaria l'adozione di misure organizzative e soluzioni tecnologiche in grado di indirizzare puntualmente la conformità con la normativa. La suite SAP Hybris include ora nuove soluzioni che supportano le organizzazioni nel centralizzare la gestione dei dati dei clienti, quali anagrafiche, canali di comunicazione preferiti, interessi relativi a prodotti e consensi alle condizioni di servizio. Al fine di realizzare un sistema centralizzato di self-service che memorizzi in modo sicuro e inviolabile le informazioni e le preferenze dei clienti, tutte le attività relative al trattamento dei dati cliente possono essere sincronizzate con le applicazioni di marketing-vendita e servizi. I nuovi regolamenti (GDPR, COPPA, privacy shield, ecc.) impongono alle organizzazioni una forte responsabilizzazione e un approccio proattivo in materia di gestione dei dati. In questa fase è quindi essenziale per le aziende dotarsi di strumenti che le possano guidare nella giusta direzione per rafforzare le relazioni di fiducia con la clientela, attraverso interazioni soddisfacenti e trasparenti.

Rosa Maria Molteni
Marketing and Communication Manager Spitch Italy Srl

Le tecnologie di identificazione e verifica di maggior impatto sono nate in tempi recenti, e si posizionano su un livello iniziale di tutela già superiore a quello stabilito dalla legge. Per esempio, le tecnologie biometriche vocali che utilizzano il linguaggio naturale (e non più la semplice password) sono strumento di verifica continua dell'identità, in maniera piacevole e insieme rigorosa dal punto di vista della compliance legale - alzando così il livello qualitativo del Customer Journey. Il focus di una soluzione innovativa di fruizione dei servizi deve essere quello di fornire strumenti di eccellenza, e non obbedire a un contesto di ottemperanza normativa. Nell'area finance - ma non solo - una soluzione/prodotto che non contenga alla base la tutela di privacy e sicurezza del cliente non può né deve essere immaginata. Queste caratteristiche rappresentano il punto di partenza di una Customer Experience realistica e utilizzabile da qualsiasi cliente, senza diffidenza nei confronti della tecnologia.