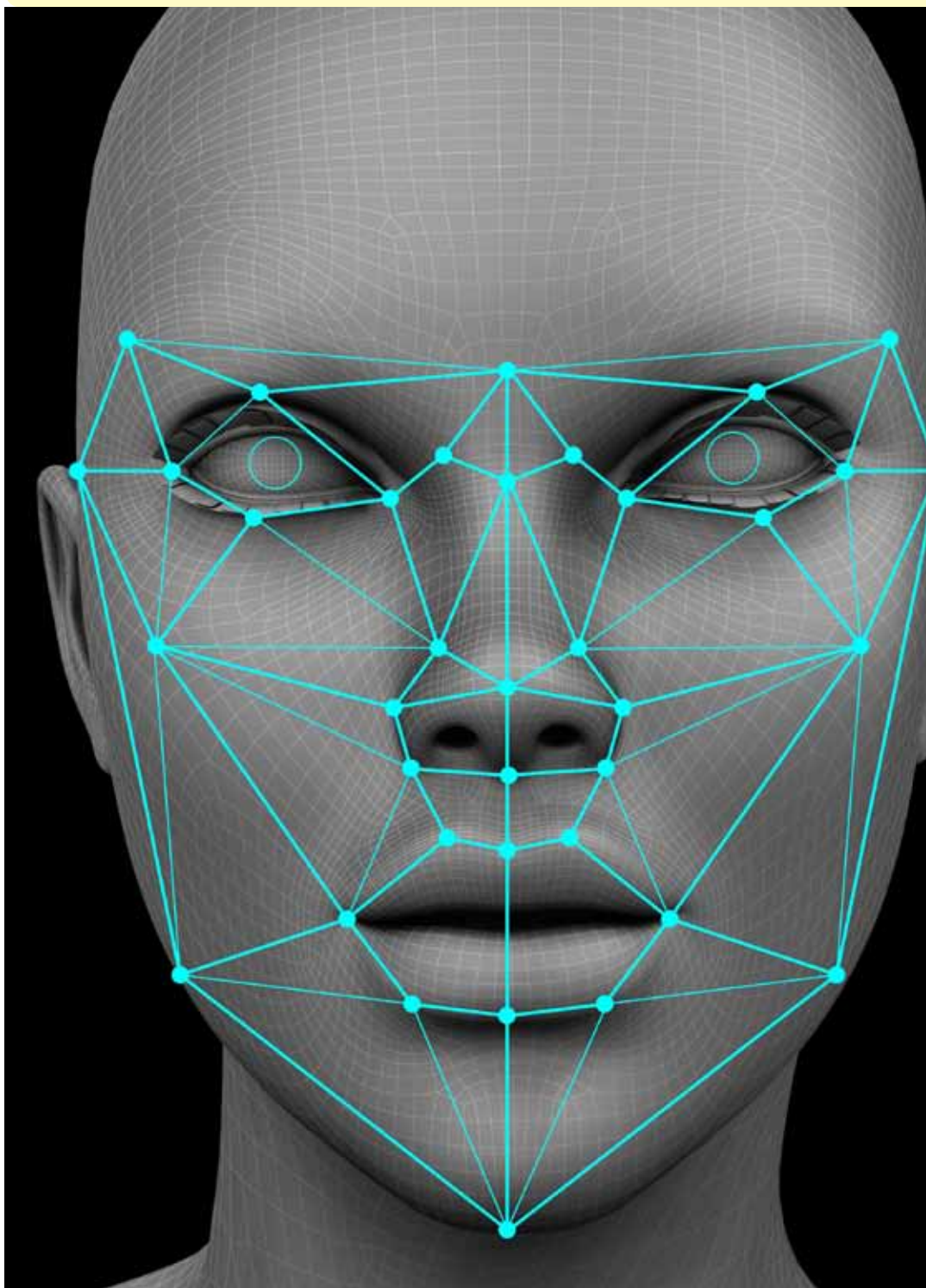


# SECURITY

& BUSINESS

n. 46



SPECIALE BIOMETRIA

Reportec

# OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID.



**Security & Business 46**  
**dicembre 2018**

Direttore responsabile:  
Gaetano Di Blasio

In redazione:  
Riccardo Florio, Giuseppe  
Saccardi, Paola Saccardi

Grafica: Aimone Bolliger

Immagini: dreamstime.com  
www.securityebusiness.it

Editore: Reportec srl  
Via Marco Aurelio 8  
20127 Milano  
tel. 02.36580441  
Fax 02.36580444  
www.reportec.it

Registrazione al tribunale  
n.585 del 5/11/2010

Tutti i marchi sono  
registrati e di proprietà  
delle relative società

Dopo una certa assenza torna Security e Business, che dal prossimo gennaio sarà una presenza costante con uscita mensile. Stiamo lavorando a un restyling grafico, ma, soprattutto a un'impostazione più snella e al contempo più ricca, grazie a nuove collaborazioni.

L'intenzione è quella di creare una newsletter mensile sulle novità più importanti del mese con contenuti esclusivi.

Viene confermata la rubrica fissa dell'associazione AIPSI (Associazione Italiana Professionisti della Sicurezza Informatica. Così come l'altrettanto storica collaborazione con il Clusit.

Siamo al lavoro per stringere ulteriori collaborazioni. Stiamo inoltre preparando l'edizione 2019 del libro "Information Security e Data Protection

Su questo numero, intanto, un interessante monito da parte di Aipsi sui rischi legati al GDPR (General Data Protection Regulation), che è ormai integrato nella legge italiana grazie al decreto Legislativo 101/2018 di armonizzazione della normativa nazionale al Regolamento Ue n. 679 del 2016, pubblicato sulla Gazzetta Ufficiale il 4 settembre 2018.

Non ci sono scuse, ma il rischio di una sanzione anche pesante, in caso avvenga una violazione dei dati informatici e non.

Il rischio maggiore è legato alla natura dei dati, in particolare quelli considerati sensibili, ma il punto critico, mette in guardia Marco Bozzetti, presidente del consiglio direttivo di Aipsi, è che spuntano esperti di GDPR come funghi, così come tanti si prestano ad assumere il ruolo di gestore dei dati, senza avere alcun titolo.

A proposito di protezione, non perdetevi lo speciale sulla biometria.

# COMPLIANCE AL GDPR: ATTENTI AGLI INCOMPETENTI E ALLE TRUFFE!

*di Marco R.A. Bozzetti, presidente AIPSI*

GDPR, General Data Protection Regulation, è il nuovo regolamento europeo sulla privacy, ed è già entrato in vigore in tutti gli stati dell'UE dal 26 maggio scorso: quindi avrebbe dovuto essere applicato ed essere operativo in ogni azienda/ente da quella data, ma ancora una non trascurabile parte degli enti e delle aziende italiane, soprattutto quelle di piccole dimensioni, sono ben lungi da un effettivo adeguamento. Anche se questo regolamento è stato approvato e rilasciato ufficialmente da ben due anni, e sono ormai 22 anni che leggi sulla privacy sono in vigore in Italia, a partire dalla 675 del 1996. La privacy e gli obblighi ad essa relativa non sono pertanto una novità, tuti dovrebbero già da tempo avere le idonee misure di protezione, ed ora semplicemente adeguarle a quanto richiesto dal GDPR, che, quale effettiva dirompente novità, prevede elevatissime sanzioni economiche:

- a) una multa fino a 10 milioni di euro, o fino al 2% del volume d'affari globale registrato nell'anno precedente nei casi di violazione degli obblighi dei titolari e dei responsabili (art. 83, Paragrafo 4)
- b) una multa fino a 20 milioni di euro o fino al 4% del volume d'affari nei casi di violazione dei principi base, dei diritti degli interessati, dei trasferimenti, degli ordini del Garante (art. 83 Paragrafi 5 e 6)

Inoltre, solo l'8 agosto scorso il Consiglio dei Ministri ha approvato il Decreto Legislativo n.101 per adeguare il quadro normativo nazionale alle disposizioni del GDPR, dopo un lungo e travagliato iter:

inviato al Parlamento il 10/5/2018 con il consenso del Garante sui suoi contenuti, e pubblicato il 4/9/2018 sulla Gazzetta Ufficiale: questo decreto è in vigore dal 19/9 scorso. Il testo del D. Lgs di adeguamento, inoltre, è di assai difficile lettura, elencando tutte le correzioni rispetto alle norme del precedente codice 196/2003 in ottica GDPR: alla faccia della chiarezza e della facile comprensione della legislazione!

Nonostante tutto, le salate multe hanno risvegliato l'attenzione sulla privacy nei vertici di aziende ed enti, ed hanno riattivato l'offerta di consulenze e di strumenti informatici di supporto.

Dati i costi e gli impegni complessivi non trascurabili per una effettiva e corretta compliance agli obblighi per la privacy, in precedenza si poteva valutare più conveniente non fare nulla, o quasi, e rischiare la piccola sanzione: ma ora? Come si comporterà l'Autorità Garante? Verranno applicate, e in che misura, le sanzioni economiche?

Nel contesto italiano, con la stragrande presenza di piccole e piccolissime imprese, a parte le ovvie eccezioni, la privacy è stata ed è considerata come uno dei tanti, troppi, obblighi burocratici costosi ed inutili, se non controproducenti, per il business e l'attività aziendale. Questo quando io azienda/ente devo trattare i dati personali dei miei interessati... Ma per me, come individuo, la protezione dei miei dati personali deve essere garantita, e bene!

Al di là di questa dicotomia, per altro riscontrabile



**SCARICA IL  
RAPPORTO  
OAD**



su vari altri temi, la privacy, di fatto sempre abbastanza trascurata dalla maggior parte dei responsabili di aziende ed enti, si rivitalizza come problema, date le possibili sanzioni. La marea di articoli, di convegni, di webinar, anche se letti a campione ed in maniera abbastanza casuale e superficiale, evidenziano come adeguare la propria situazione della privacy al GDPR non sia una passeggiata e richieda comunque un impegno non trascurabile che coinvolge anche il vertice dell'organizzazione.

Di conseguenza le domande tipiche che si pongono i decisori di vertice: forti sanzioni? Ma quando mai verranno a controllarmi? Ho ben altre spese cui far fronte! Sicurezza digitale? Ho già l'antivirus e il controllo degli accessi ... Il resto è troppo complicato e costoso e poi chi mai vorrà attaccarmi digitalmente? E con questo in mente, contatta persone di fiducia e si informa su quello che fanno aziende/enti simili alla sua. Sovente senza aver ben compreso che cosa richiede il GDPR, entra in contatto con suoi, e

di altri, professionisti, tipicamente commercialisti, avvocati, consulenti del lavoro, fornitori di informatica, consulenti ed altri “specialisti”. Ed entra così in ginepraio di suggerimenti, proposte ed offerte dal quale, se non ha un minimo di conoscenza su privacy e sicurezza digitale, avrà difficoltà ad uscirne “vivo” col minimo dei danni.

Moltissimi dei professionisti che si propongono in tema di privacy e di adeguamento al GDPR sono seri ed affrontano correttamente ed eticamente il problema. Ma purtroppo sul mercato italiano è in forte crescita l’offerta di servizi per la privacy “chiavi in mano” a prezzi ridicoli, che non possono che offrire soluzioni e documenti generali e non contestualizzati sulla realtà del cliente. Giocoforza tali soluzioni costituiscono una insufficiente copertura e sono soldi mal spesi, anche se pochi: la responsabilità è del legale rappresentante della azienda/ente, e non ne risponde, in prima battuta, il consulente e/o il fornitore. Per la sicurezza digitale poi, molti fornitori di informatica vendono le soluzioni che hanno, trascurando le effettive necessità del cliente ed approfittando della incompetenza sua e dei suoi collaboratori. Privacy e sicurezza digitale sono multi-disciplinari e richiedono una vasta gamma di competenze e di esperienza sul campo. Difficilmente un’azienda/Ente, soprattutto se piccola, può avere al proprio interno specifiche e aggiornate competenze di privacy e sicurezza digitale. Deve pertanto terziarizzare gran parte (o la totalità) delle decisioni e dell’operatività, e l’unico criterio di scelta è spesso il passa parola ed il costo. Ma di chi si può fidare?

Come può garantirsi sulle reali competenze dei fornitori e dei consulenti? Il problema è il medesimo per la scelta dei professionisti di riferimento, quali i commercialisti, i fiscalisti, gli avvocati e così via. Un primo suggerimento in merito nella scelta è il verificare per la persona e/o per l’azienda, quale condizione necessaria ma non sufficiente:

- l’averne una o più certificazioni sulla privacy e sulla sicurezza digitale, in particolare le uniche con valore legale europeo: eCF - EN 16234 1:2016 (Per approfondimenti si veda il sito <https://www.aipsi.org/aree-tematiche/crescita-e-percorsi-professionali.html>)



- l'appartenenza ad una o più associazioni professionali esistenti in Italia per la privacy e la sicurezza digitale.

### **Alcune considerazioni conclusive:**

- GDPR lascia alla responsabilità del titolare l'individuazione delle idonee misure di sicurezza digitale, a seguito dell'Analisi dei rischi, ma evidenzia la necessità/opportunità di criptare i dati personali, e di individuare data breach;
- L'adeguamento al GDPR è un obbligo serio da non sottovalutare, che deve coinvolgere il personale interno dell'azienda/ente e che richiede
  - misure di tipo organizzativo, sia verso l'interno sia verso le Terze Parti coinvolte
  - misure di tipo tecnico quali l'analisi dei rischi e degli impatti, Architetture, tecniche e strumenti di sicurezza digitale, in primis la crittografia dei dati critici e sensibili, misure di sicurezza fisica per gli archivi cartacei, etc.
  - Misure di governance, con sistematico monitoraggio e controllo delle misure in atto, per rispondere al principio di accountability e di inversione dell'onere della prova, e che richiedono anche una idonea documentazione degli interventi effettuati o a piano.
  - Tutte le aziende/enti sono sempre più a rischio digitale, indipendentemente dalle loro dimensioni e dal settore merceologico di appartenenza.
  - L'idonea sicurezza digitale è necessaria non solo e non tanto per adempiere agli obblighi della privacy, ma per garantire la continuità operativa dell'organizzazione, che ormai dipende quasi interamente dal supporto informatico.
  - Privacy, GDPR e sicurezza digitale hanno dei costi non trascurabili, ma quali sono i costi della "non privacy" e della "non sicurezza digitale"?



**SPECIALE**

# SOLUZIONI CHE SFRUTTANO I PARAMETRI BIOMETRICI





PAPILÁRA 1 x456zk  
0078% 046mm  
markant OK

PAPILÁRA 2 x395zk  
0086% 046mm  
markant OK

PAPILÁRA 3 x534pk  
0087% 042mm  
markant OK

*Diverse e uniche sono le  
caratteristiche che rendono  
univocamente identificabile  
un individuo*

## UN AMBIENTE DI LAVORO PROTETTO IN PALMO DI MANO



*Biometria, servizi per la gestione di credenziali e privilegi d'accesso per la certezza dell'autenticazione con Fujitsu*

*di Gaetano Di Blasio*

**G**li strumenti digitali rendono sempre più efficiente il lavoro degli information worker ma la tecnologia deve stare al passo con le nuove esigenze di flessibilità pretese dagli utilizzatori abituati a un uso dinamico di dispositivi mobili e applicazioni web.

Di fatto, possiamo osservare che gli utenti hanno accesso a molteplici sistemi e piattaforme varie. Per una massima efficacia e una maggiore efficienza, è importante che i dati giusti arrivino all'utente giusto, affinché possa svolgere il proprio lavoro al meglio. Ma non è solo una questione di produttività: si pone, infatti un cruciale problema di fiducia.

Fiducia, che verrebbe meno se non si avesse la certezza dell'identità di un utente con il quale si vuole comunicare, collaborare, chiudere una transazione e così via.

Con Workplace Protect AD (WPP AD), Fujitsu estende la propria suite per la protezione e l'autenticazione dell'identità digitale, basata sulla tecnologia PalmSecure.

Il software WPP AD abilita un sistema di accesso basato su Active Directory Windows a riconoscere i log-in con PalmSecure, attraverso qualsiasi rete.

### **L'autenticazione biometrica**

La soluzione proposta, come accennato, espande la suite di autenticazione Fujitsu. Workplace Protect AD, infatti, sostituisce il login realizzato attraverso credenziali del provider Windows, mentre l'uso di PalmSecure con verifica biometrica sostituisce la password.

Le informazioni di autenticazione sono decifrate e passate all'Active Directory, se vengono abbinate a un template valido del palmo equindi riconosciute. Per questo gli utenti dovranno essere registrati centralmente per ogni tipo di sensore PalmSecure che dovessero utilizzare. Infine, i modelli biometrici saranno memorizzati nell'Active Directory Service dell'impresa.

Una volta registrati, gli utenti potranno autenticarsi con uno username e con il palmo della mano in tutti i domini dell'organizzazione innalzando il sistema di sicurezza.

Il login biometrico è molto più sicuro di quello basato su una password, che è a volte facile da indovinare, quando non è scritta su un post-it attaccato allo schermo del pc o letta da un collega "curioso" mentre viene digitata.

Anche dando ingenuamente per scontato che questi comportamenti appartengono al passato e che tutti sono più consapevoli dei rischi, ci sono cyber criminali in grado di "hackerare" anche le password più lunghe e complesse. Senza dimenticare i PIN di molti dispositivi basati su card, magari contact

less, che sono tra i principali punti deboli per quanto riguarda i furti d'identità, come evidenziano i manager di Fujitsu.

Per questo Fujitsu ha progettato la tecnologia Palm-Secure, che riconosce il disegno dei vasi sanguigni del palmo e non "semplicemente" un'impronta digitale. Da notare che il palmo non viene poggiato su alcuna superficie, quindi non ci sono problemi igienici. Ma non solo: per prevenire azioni estreme degne dei thriller di Quentin Tarantino, il sistema consente l'accesso solo se rileva il sangue scorrere nelle vene. L'affidabilità di riconoscimento, spiegano presso Fujitsu, è garantita dall'utilizzo di oltre 5 milioni di punti di riferimento che vengono mappati.

### **L'identità come servizio: Fujitsu IDaaS**

È chiaro che questi dati devono essere gestiti con molta attenzione, altrimenti potrebbero finire in mano a malintenzionati, creando all'impresa grossi problemi, danni e perdita di denaro.

Fujitsu, che si occupa di ID management da decenni, ha ideato un servizio chiamato Fujitsu IDaaS (Identity as a Service), che è stato progettato per tenere sotto controllo e gestire in sicurezza le identità digitali degli utenti aziendali.

Il sistema è centrato sull'utente, in modo da massimizzare la sua experience. Del resto, le strutture, i modelli e gli ambienti d'organizzazione in un'impresa sono costantemente in evoluzione. Oggi, infatti, è usuale acquistare applicazioni web o servizi online, talvolta anche solo attivare un "trial" gratuito in cloud. Ciò determina generare username (spesso la mail aziendale) e password (magari sempre la stessa). Credenziali che vengono abbandonate se la prova non soddisfa le aspettative, ma restano sui sistemi.

### **Una gestione efficace**

La criticità nella gestione delle identità digitali si accompagna frequentemente con oneri e costi elevati. La soluzione proposta da Fujitsu mette a disposizione delle imprese un servizio completo di identity management basato sulle identità già adottate. Le credenziali già in uso vengono salvate e mantenute nella directory dell'impresa, cui il sistema di Fujitsu si collega attraverso interfacce open standard.

In questo modo le imprese potranno utilizzare funzionalità avanzate di deployment e gestione end-to-end delle identità, quali: creazione, modifica e rimozione delle autorizzazioni previste per ogni utente, gestibili anche con interfacce self-service, impostando una procedura per l'approvazione dei privilegi.

Ovviamente sta all'impresa decidere se assegnare la gestione a un help desk.

Le modalità di autenticazione previste sono diverse, da quelle più semplici alle varie possibilità di strong authentication. Molto utile è il single sign-on, che semplifica il lavoro all'utilizzatore finale e riduce gli oneri di gestione per ogni account.

La scalabilità è un'ulteriore caratteristica che differenzia il servizio e permette di aggiungere per ciascun utente, elementi distintivi, come per esempio privilegi e la loro gestione oppure il single sign on. Il servizio può essere gestito interamente da remoto via Web e non richiede l'installazione di client.

Qualora si volesse integrare in servizio in piattaforme aziendali, come accennato sono disponibili strumenti open standard, come, per esempio, open SOA SAML (Security Assertion Markup Language), WS-Federation (Web Services Federation).

# VOLTAGE SECUREDATA: IL CICLO DI VITA PER I DATI CIFRATI

*Grazie a una serie di tecnologie di cifratura innovative e a un portfolio di soluzioni ritagliate per ogni specifica esigenza, Micro Focus propone un approccio dato-centrico che garantisce completa protezione dei dati nel loro intero ciclo di vita*

*di Riccardo Florio*



L'esplosione di informazioni, normative e regolamenti e della complessità associata rende più difficile per l'IT proteggere i dati aziendali e personali in modo efficace e amplia la superficie di attacco. Tutto ciò rende più semplice per i criminali informatici individuare, sottrarre, diffondere o distruggere i dati la cui perdita rappresenta la principale fonte di costo totale subito da un'azienda.

## **Una sicurezza dato-centrica**

Le soluzioni di cifratura sono un requisito irrinunciabile, ma quelle di tipo tradizionale non garantiscono una protezione costante dei dati in ogni momento del loro ciclo di vita e in qualsiasi stato si rovino: a riposo, in movimento e in uso da parte di un'applicazione.

Micro Focus supera questo ostacolo tramite le soluzioni Voltage SecureData, sfruttando un approccio di sicurezza "data centrico" che prevede di implementare il meccanismo di difesa e protezione

direttamente sul dato o sui sistemi che lo trattano. Alla base di questo approccio vi sono una serie di tecnologie specifiche e brevettate di cifratura e tokenizzazione (un processo che sostituisce il dato in ingresso con un token generato casualmente che "rappresenta" il dato stesso) che rendono i dati inutilizzabili anche nel caso di sottrazione.

## **Cifratura che non penalizza l'uso dei dati**

Hyper Format-Preserving Encryption (Hyper FPE) crittografa i dati sensibili, preservando il formato originale e quindi l'integrità referenziale, senza ridurre il livello di protezione. Questo permette alle applicazioni, ai processi di analytics e ai database di utilizzare i dati protetti senza alterazioni, anche attraverso sistemi, piattaforme e strumenti distribuiti. Questo requisito è importante anche quando si devono gestire insiemi di dati inseriti in Hadoop e ancor più critico quando vengono utilizzati identificatori comuni come il codice fiscale o la carta

di identità come riferimenti comuni tra insiemi di dati diversi.

**Embedded Format-Preserving Encryption (eFPE)** è una tecnologia che effettua la cifratura del dato in modo che nel "ciphertext" siano integrati i dati dell'identità mantenendo la stessa lunghezza ma non il set di caratteri del dato in ingresso (che invece viene mantenuto in Hyper FPE).

### Tecnologie che fanno la differenza

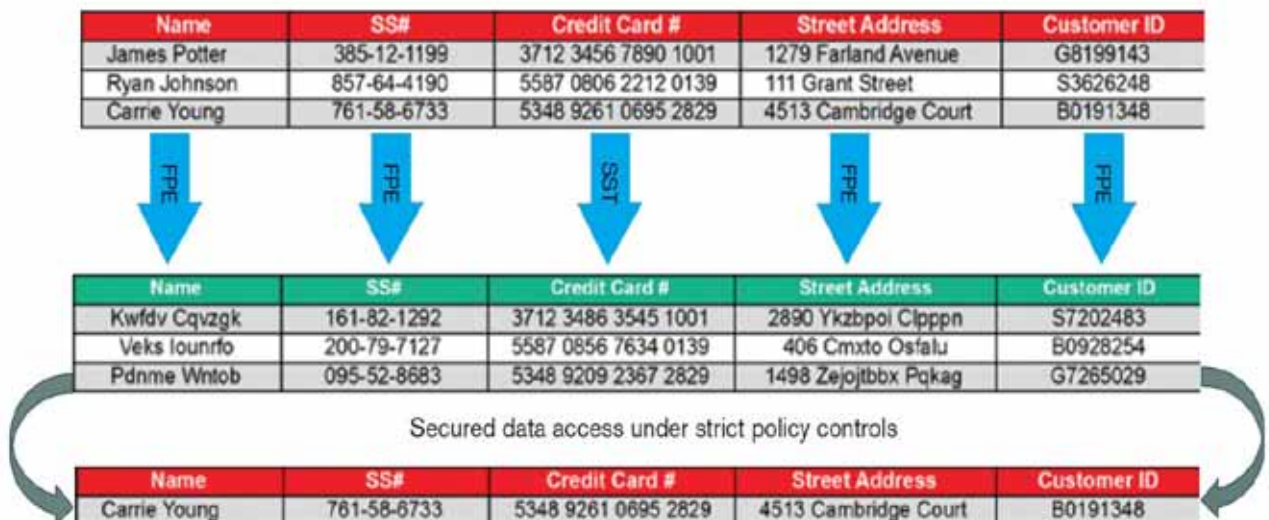
Un'altra tecnologia brevettata e innovativa per la sicurezza dei dati delle carte di pagamento utilizzata dalle soluzioni Voltage SecureData è **Hyper Secure Stateless Tokenization (Hyper SST)**. Questa tecnologia elimina il database dei token, che è invece centrale per altre soluzioni di tokenizzazione, e rimuove la necessità di memorizzare i dati del titolare della carta o altri dati sensibili. Questo migliora la velocità di conversione, la scalabilità (senza introdurre alcun degrado con la crescita), la sicurezza, la gestibilità del processo di tokenizzazione e riduce i costi.

**Identity-Based Encryption (IBE)** è una soluzione di crittografia end-to-end che prevede che la

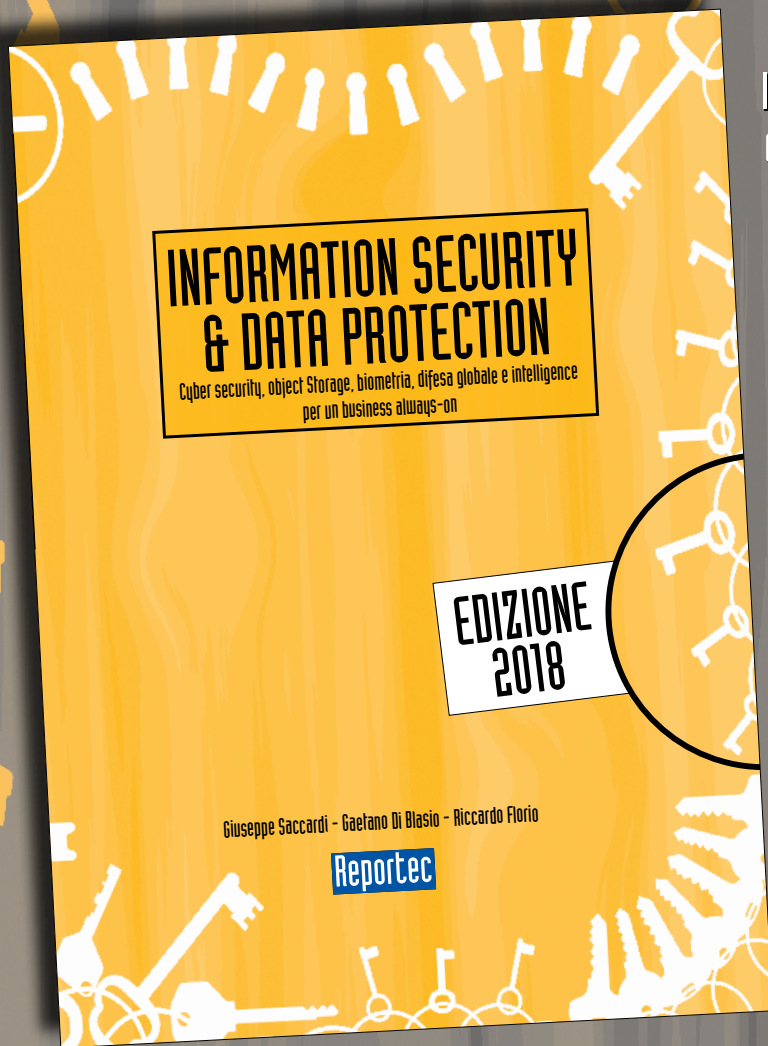
cifratura e l'identità seguano il dato stesso in modo che le applicazioni possano accedervi direttamente senza gestire chiavi e certificati. In tal modo, elimina la complessità dei tradizionali sistemi di infrastruttura a chiave pubblica (PKI) e dei sistemi a chiave simmetriche con i relativi costi di creazione e manutenzione.

**Stateless Key Management** abilita un processo di generazione e rigenerazione della chiave di cifratura di tipo on-demand, senza la necessità di dover mantenere un archivio delle chiavi destinato a continuare a crescere. Il risultato è un sistema che può essere scalato infinitamente tra posizioni fisiche e logiche distribuite, riducendo sensibilmente i costi IT e facilitando l'amministrazione.

**Page-Integrated Encryption (PIE)** cifra i dati sensibili dell'utente nel browser e permette che vengano cifrati attraverso livelli intermedi dell'applicazione. A differenza della tradizionale crittografia TLS/SSL, questo meccanismo mantiene i dati dell'utente privati durante lo spostamento attraverso i sistemi di bilanciamento del carico e gli "stack" delle applicazioni Web e provvede a decifrarli solo quando raggiungono i sistemi host interni sicuri.



# È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

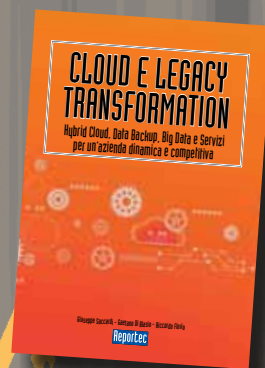


In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business.

Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate.

Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.

È disponibili anche  
**CLOUD E LEGACY TRANSFORMATION**



Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a  
**info@reportec.it - tel 02 36580441 - fax 02 36580444**