


SPECIALE

LA BIOMETRIA PER UN'IDENTITÀ SICURA



Anche la moda dei dispositivi indossabili sta spingendo la ricerca verso lo sviluppo di soluzioni che utilizzano i parametri biometrici, univoci per ciascun individuo, al fine di realizzare soluzioni per l'autenticazione dell'identità semplici e affidabili.

pag. 8-17

CYBER ATTACK

FURTO DI DATI: IL PERICOLO È INTERNO

Le violazioni alla sicurezza informatica che hanno successo, nella stragrande maggioranza dei casi, sono favorite dal comportamento scorretto di un dipendente. Un fatto noto da tempo, ma stupisce il risultato di un nuovo rapporto realizzato da HfS Research per conto di Accenture, secondo il quale, ben il 69% dei manager intervistati ha dichiarato di aver riscontrato, negli ultimi dodici mesi, furti o tentativi di furti, nonché corruzioni dati, da parte di insider.

pag. 4

PROTAGONISTI

GASTONE NENCINI, TREND MICRO: SOCIAL: UN RISCHIO DA GESTIRE

La pubblicazione di informazioni, foto e video personali sui social network offre innumerevoli opportunità al cybercrime per violare la nostra privacy, sottrarre dati personali e causare danni economici. Poche semplici regole riducono molto i rischi.

pag. 19



IN QUESTO NUMERO:

OPINIONE

pag. 3

- La questione culturale e il bisogno di semplicità

CYBER ATTACK

pag. 4

- Furto di dati: il pericolo è interno

SPECIALE

pag. 9

- La sicurezza e i dati biometrici
- pag. 11*
- Pagamenti sicuri con i dati biometrici: il sì degli europei
- pag. 14*
- Biometria e legge: istruzioni per l'uso

SOLUZIONI

pag. 18

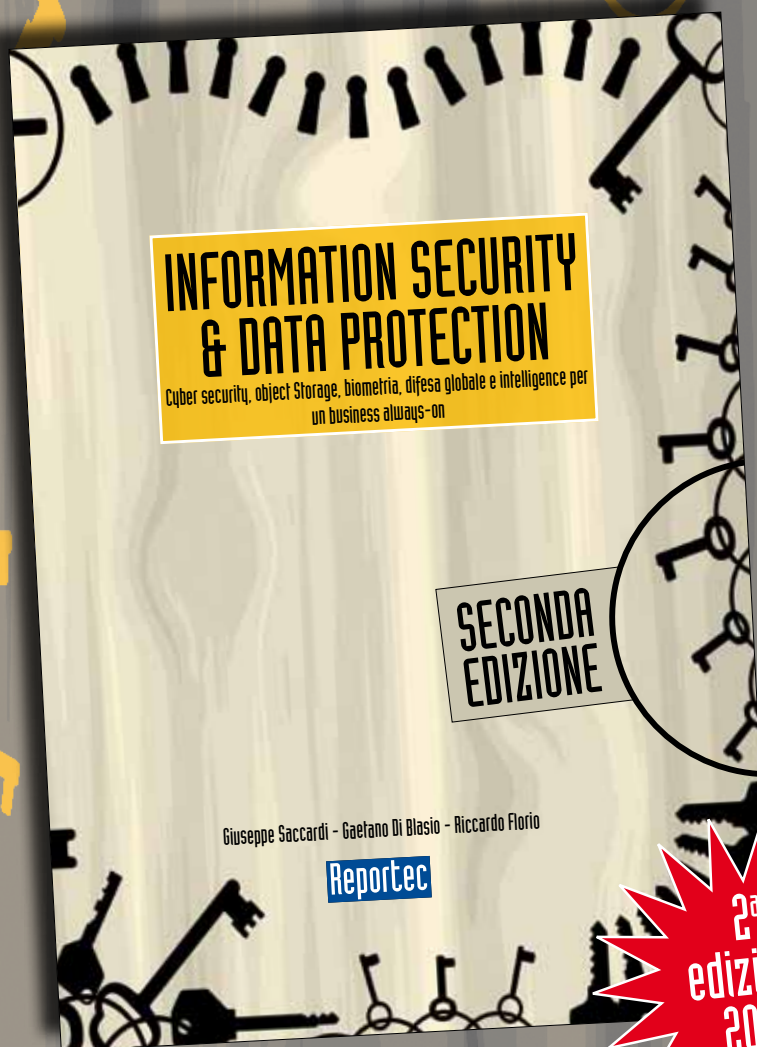
- Security testing con il nuovo team Ibm X-Force Red

PROTAGONISTI

pag. 19

- Gastone Nencini, Trend Micro. Social network: un rischio da gestire

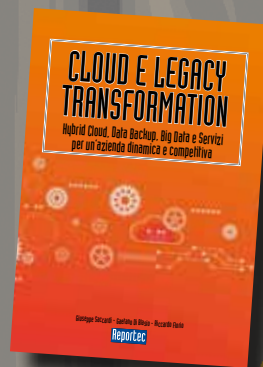
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



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.

2^a
edizione
2016

È disponibili anche
CLOUD E LEGACY TRANSFORMATION



Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

LA QUESTIONE CULTURALE E IL BISOGNO DI SEMPLICITÀ

In cyber attack di questo mese, un report realizzato per conto di Accenture mette l'accento sul rischio proveniente dai dipendenti. Sono sempre loro la causa principale delle violazioni alla sicurezza informatica. Lo hanno capito i manager aziendali, anche sulla propria pelle, ma non basta ad aumentare gli investimenti in cyber security e, in particolare, in competenze e talenti.

Una vecchia storia che si ripete e che non sembra possa trovare uno sbocco. Eppure la strada deve essere trovata e va cercata negli automatismi che possono guidare l'utente e aiutarlo a non sbagliare. Formazione e cultura e ancora cultura e formazione. Un mantra da ripetere per impedire che si clicchi su un link in una mail che non provenga da una fonte ben conosciuta, senza prima chiedersi: è possibile che questa mail sia falsa?

Come emerge da una ricerca di Visa, di cui diamo ampio resoconto nello speciale sulla sicurezza biometrica, gli individui sono attenti alla sicurezza quando ci sono di mezzo i soldi: più precisamente per quanto concerne i metodi di pagamento. Ma, anche in questo caso, cercano soluzioni che siano semplici.

Cercare la via più semplice è una costante della natura e, come esseri umani, siamo anche noi portati a scegliere le soluzioni più rapide e facili. Tale considerazione deve essere sempre nella mente di chi progetta le soluzioni per la sicurezza e di chi configura le security policy aziendali e i sistemi di enforcement delle stesse.

Restando nell'ambito della biometria, la propensione degli italiani per i pagamenti autenticati con sistemi a due fattori, di cui uno basato su parametri biometrici può senz'altro essere sfruttata per aumentare le vendite e i clienti, accogliendoli con sistemi che soddisfano il loro bisogno di semplicità, ma gli interessati faranno bene a valutare gli aspetti legali, ben argomentati dall'avvocato Abeti, sempre nello speciale di copertina.

Security & Business 37
luglio-agosto 2016

Direttore responsabile:
Gaetano Di Blasio

In redazione:
Riccardo Florio, Giuseppe
Saccardi, Paola Saccardi,
Daniela Schicchi

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

FURTO DI DATI: IL PERICOLO È INTERNO

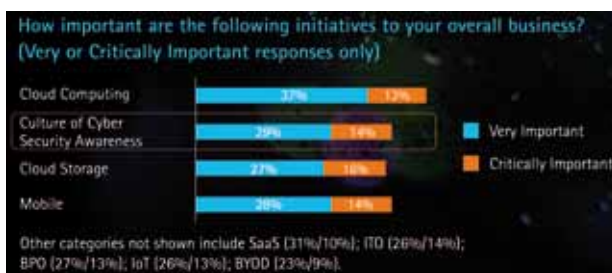
Un report di Accenture e HfS mostra che le maggiori preoccupazioni riguardano i dipendenti infedeli. Troppo pochi i fondi per assumere e mantenere esperti di sicurezza informatica

di Gaetano Di Blasio

Le violazioni alla sicurezza informatica che hanno successo, nella stragrande maggioranza dei casi, sono favorite dal comportamento scorretto di un dipendente. Un fatto noto da tempo, ma stupisce il risultato di un nuovo rapporto realizzato da HfS Research per conto di Accenture, secondo il quale, ben il 69% dei manager intervistati ha dichiarato di aver riscontrato, negli ultimi dodici mesi, furti o tentativi di furti, nonché corruzioni dati, da parte di insider. Certo, una parte dei comportamenti sono stati compiuti per disattenzione o per aver ignorato policy di sicurezza, sottovalutandone l'importanza, ma molte sono riferibili a veri e propri casi d'infedeltà. La percentuale più alta è stata registrata dalle organizzazioni attive nell'ambito dei media e della tecnologia (77%).

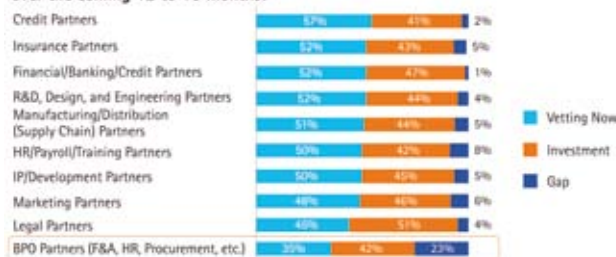
In base alle considerazioni degli esperti di sicurezza, questo tipo di rischi sarà difficile da debellare, anzi l'opinione espressa dagli autori del report è che il furto di informazioni aziendali da parte di personale interno possa aumentare di quasi due terzi nei prossimi 12 o 18 mesi. Più precisamente, nonostante la disponibilità di soluzioni tecnologiche avanzate, quasi la metà di tutti i rispondenti dichiara preoccupazioni rilevanti circa il furto di dati da parte di personale interno (48%) e gli attacchi malware (42%) nei prossimi 12 o 18 mesi.

Ma c'è un altro risultato dell'indagine "The State of Cybersecurity and Digital Trust 2016" che preoccupa di più: la carenza di budget per investire nell'assunzione di dipendenti opportunamente formati e



Il cloud spinge la digital transformation (fonte Accenture e HfS)

Do you have a mechanism or set of policies (SOP) to vet ecosystem partners for their own cyber-integrity and preparedness, and where do you expect to invest over the coming 12 to 18 months?

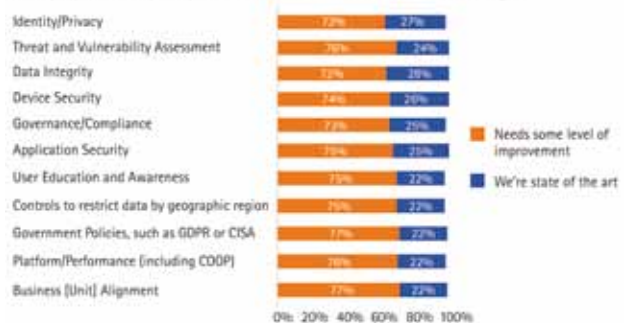


Il parity gap rilevato dai ricercatori (fonte "The State of Cybersecurity and Digital Trust 2016" di Accenture e HfS)

di talenti in ambito di cyber security. Alla domanda sull'attuale situazione in termini di finanziamenti e personale, il 42% circa dei rispondenti ha riferito l'esigenza di un aumento dei fondi per l'assunzione di professionisti di sicurezza informatica e la formazione. Oltre la metà dei rispondenti (54%) ha aggiunto che gli attuali dipendenti non sono sufficientemente preparati per prevenire il verificarsi di violazioni della sicurezza e le cifre sono solo lievemente migliori in termini di rilevamento (47%) e risposta (45%) agli incidenti.

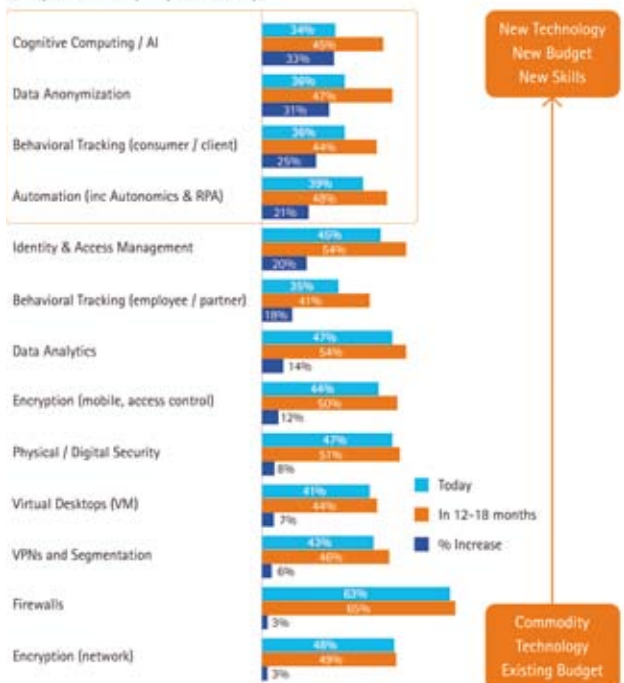
- Tale insufficienza impedisce alle organizzazioni di difendersi adeguatamente dagli attacchi, ma è solo uno su quattro lacune significative che pregiudicano la capacità delle imprese di contrastare o mitigare efficacemente attacchi cibernetici mirati e ben organizzati:
- **Competenze e budget:** secondo il 31% degli intervistati, l'unico e principale inibitore nella lotta contro gli attacchi è la mancanza di fondi da investire nella formazione o nel personale. Inoltre, il 70% dei rispondenti riferisce una mancanza o un'inadeguatezza dei fondi da investire in tecnologia per la cyber security o nei talenti in ambito di sicurezza, inclusa la loro formazione.

How prepared are you [your staff] to handle each of the following?



Capacità e limiti di risposta (fonte Accenture e HfS)

Please indicate how important you feel each of the following technologies are today and how important they will be within 12 to 18 months (Very or Critically Important only)



Il Technology gap (fonte Accenture e HfS)

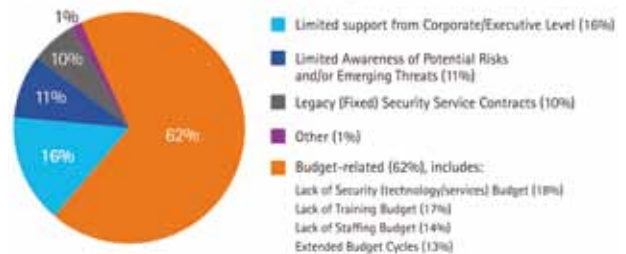
- **Tecnologia:** nei prossimi 12 o 18 mesi è previsto un significativo aumento nell'impiego di applicazioni riguardanti cognitive computing e intelligenza artificiale (31%) e di piattaforme per la cifratura dei dati (25%).
- **Parità:** il livello di sicurezza di un'impresa è pari a quello dell'anello più debole della catena, cioè il proprio partner meno sicuro, eppure le aziende che hanno dichiarato di porre attenzione e valutare la preparazione e l'integrità informatica dei partner del proprio ecosistema vanno dal 35% al 57% per le varie tipologie di soggetti con i quali interagiscono. In particolare, i partner di Business Process Outsourcing risultano essere quelli meno controllati (35%), mentre l'attenzione principale è rivolta alla verifica dei partner in ambito creditizio (57%)
- **Management:** mentre il 54% dei rispondenti è d'accordo o fortemente d'accordo sull'efficacia della cybersecurity per creare fiducia digitale tra i consumatori, il 36% ritiene che l'Executive Management la consideri una spesa superflua.

Lo studio è stato eseguito su oltre 200 executive in ambito security di alto livello e altri professionisti IT appartenenti a diverse aree geografiche e diversi settori industriali.

Dopo aver analizzato lo stato attuale e futuro della cyber security nelle aziende, la ricerca ha quindi preso in esame le misure necessarie a favorire lo sviluppo di una fiducia digitale nell'intero ecosistema in cui l'azienda opera.

Siamo ormai prossimi a essere travolti dall'onda del business digitale e i risultati del report mostrano le

Which of the following are the biggest inhibitors to your organization's security provision? (single biggest inhibitor)



Source: "The State of Cybersecurity and Digital Trust 2016" Accenture and HfS Research - Sample: 208 Enterprise Security Professionals

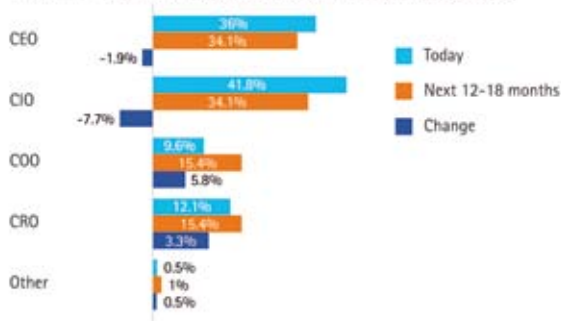
I freni agli investimenti in sicurezza (fonte Accenture e HfS)

lacune significative tra offerta e la domanda di talenti. A preoccupare non è solo la carenza di budget in se, ma anche altre conseguenze della stessa, a cominciare dal divario che si crea tra le aspettative del Management e i team che si occupano di sicurezza.

Metodologia dello Studio Accenture - HfS Research

Tra marzo e maggio 2016 HfS Research e Accenture hanno condotto un sondaggio combinato di tipo quantitativo e basato su interviste a 208 professionisti di enterprise security in sette settori e attraverso una vasta gamma di segmenti verticali. Oltre due terzi di tutti i rispondenti (68%) erano dirigenti di alto livello con compiti di supervisione della sicurezza delle rispettive organizzazioni. Il 29% è stato selezionato in Nord America, il 30% nell'EMEA, il 30% nell'APAC e l'11% in America Latina. Per maggiori informazioni www.accenture.com/cybersecurity2016.

Which of the following best describes your Security Management Reporting Structure today, and how do you believe it should change within 12-18 months? (data shows % of reporting lines)



La struttura aziendale di gestione del rischio cyber (fonte Accenture e HfS)

Oltre le lacune

Paolo Dal Cin, Managing Director di Accenture Security, afferma: «La nostra ricerca evidenzia diversi punti di riflessione. Coloro che gestiscono la sicurezza in azienda ritengono che le minacce non sono in diminuzione, bensì in aumento, e si aspettano sempre maggiori ostacoli per la protezione di dati critici e la creazione di un clima di fiducia digitale». Allo stesso tempo, aggiunge il direttore, «le organizzazioni vogliono investire in tecnologie informatiche avanzate, ma non possiedono fondi a sufficienza per assumere o formare personale competente in grado di utilizzarle in modo efficiente».

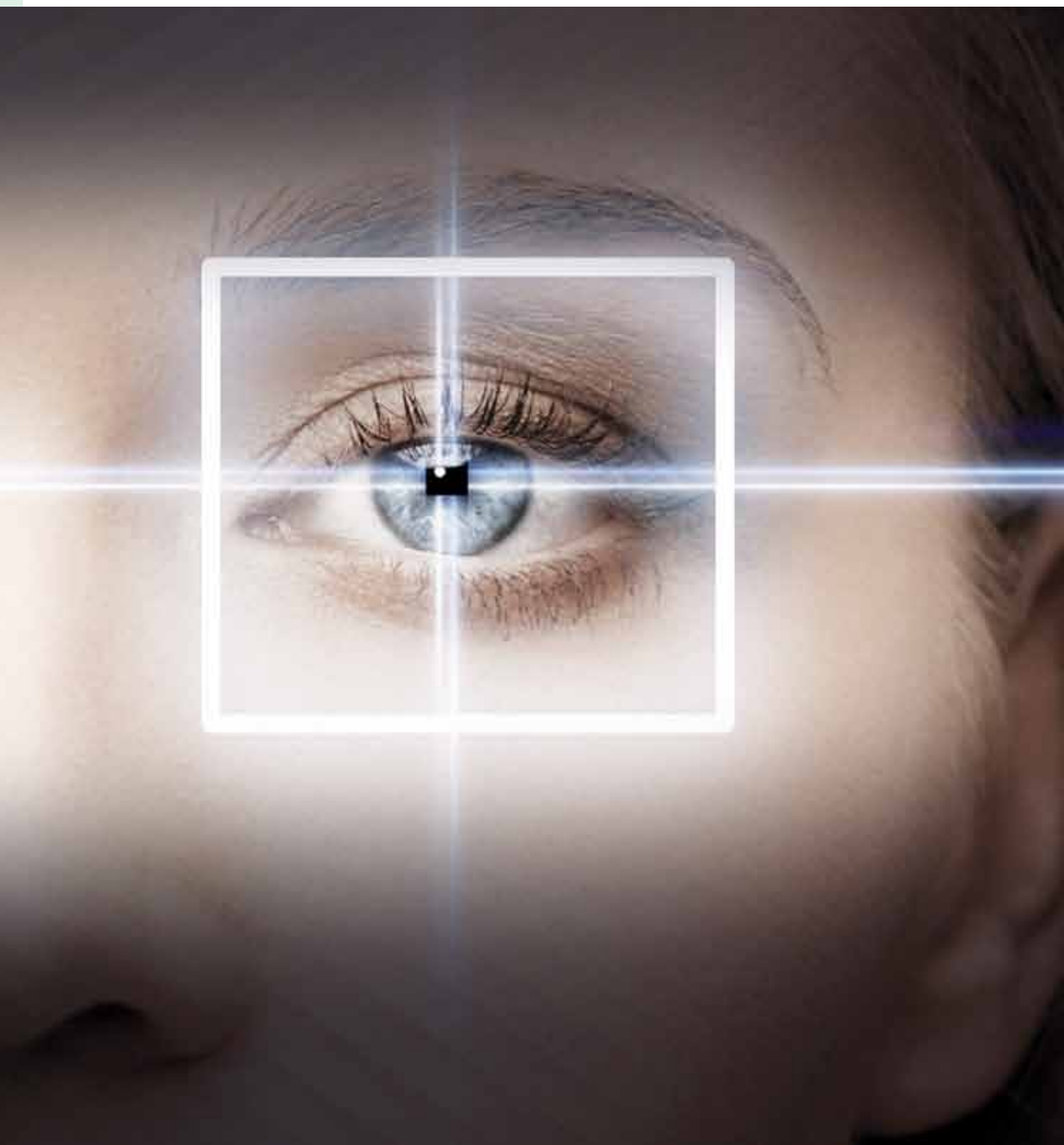
La conclusione di Dal Cin è: «Per fronteggiare il problema della sicurezza le imprese dovranno necessariamente collaborare con un ecosistema aziendale esteso, costituito dalle diverse business unit, partner, provider e utilizzatori dei servizi, con l’obiettivo di creare un ambiente di fiducia digitale».

«Le lacune identificate possono essere colmate. Tuttavia rivelano la necessità di un approccio diverso,

che includa misure di gestione del rischio più rigorose e preveda lo sviluppo di un clima di fiducia digitale», sostiene Fred McClimans, vice-presidente per la Ricerca, settore Digital Trust and Cybersecurity diHfS Research, che conclude: «A tale scopo, un’importante opportunità consiste nel ripensare a come integrare fiducia digitale e sicurezza nel tessuto aziendale, adottando soluzioni di automazione e di Artificial Intelligence, oltre che collaborazioni con partner esterni».

SPECIALE

**LA SICUREZZA
E I DATI BIOMETRICI**



Continua a crescere la tendenza a studiare sistemi di autenticazione basati su parametri legati alla persona, ma non mancano note dolenti

Anche la moda dei dispositivi indossabili sta spingendo la ricerca verso lo sviluppo di soluzioni che utilizzano i parametri biometrici, univoci per ciascun individuo, al fine di realizzare soluzioni per l'autenticazione dell'identità semplici e affidabili.

Mentre si parla di dispositivi sottocutanei di prossima generazione, si diffondono soluzioni che sfruttano scansioni di iride o impronte digitali per garantire il riconoscimento dell'utente. Nelle prossime pagine, una ricerca commissionata da Visa, mostra come tali sistemi, abbinati ad altri elementi per una strong authentication a due fattori, siano ben visti e considerati sicuri dai consumatori europei e italiani soprattutto. Una confidenza tutto sommato ben riposta per i sistemi studiati per il controllo fisico degli accessi, per esempio ad aree specifiche, o per l'attivazione di macchinari. Sistemi sicuri sono anche quelli usati per di tipo logico, cioè per l'autenticazione informatica. Tali sistemi impiegano i parametri biometrici, come impronte digitali, lineamenti del volto, immagine della retina o dell'iride, timbro vocale, struttura venosa delle dita, geometria della mano e altri, per autenticare un individuo tramite comparazione con un modello registrato in precedenza.

Tale modello consiste comunque in un codice binario che sarà memorizzato in un database. Come tale non è immune dal rischio di essere copiato per scopi illeciti. In questo caso, il problema è anche che si verifichino effetti lesivi rilevanti e duraturi poiché, diversamente dai sistemi di autenticazione

tradizionali, diventa impossibile fornire alla vittima del furto una nuova identità biometrica che utilizzi la stessa tipologia di dato biometrico.

I fattori di scetticismo

Il caso estremo esposto è solo uno degli esempi portati da chi si oppone all'utilizzo dei dati biometrici. Quest'ultimo, infatti, dato l'elevato grado di unicità nella popolazione di molte caratteristiche biometriche, espone al rischio che soggetti privati e istituzioni possano acquisire informazioni sui singoli individui per finalità differenti da quelle per cui tali dati biometrici sono stati in origine raccolti, incrociando e collegando dati provenienti da più banche dati.

Peraltro, alcune caratteristiche biometriche possono essere acquisite senza la consapevolezza o la partecipazione di un individuo.

Inoltre, va ricordato che il riconoscimento biometrico avviene generalmente su base statistica e non deterministica e, pertanto, non è esente da possibili errori. In generale, i sistemi in commercio dichiarano il tasso di errore dei due tipi e sarà l'impresa utilizzatrice a dover scegliere quale dei due rischi è il meno grave, ma prima dovrà attentamente valutare se l'uso dei dati biometrici siano necessario, perché l'Unione Europea è incline a introdurre limitazioni, peraltro già presenti nel codice italiano della Privacy (si veda anche l'articolo sulle questioni legali nelle prossime pagine).

L'attenzione delle autorità è a favore del cittadino e, al momento sembra favorire approcci conservatori.



PAGAMENTI SICURI CON I DATI BIOMETRICI: SI DAGLI EUROPEI

Due terzi dei consumatori nel vecchio continente sono propensi a utilizzare la biometria per i pagamenti e tre quarti ritengono sicura l'autenticazione biometrica in combinazione a un dispositivo fisico.

di Gaetano Di Blasio

Il 68% dei consumatori europei, oltre due terzi, si esprimono positivamente riguardo l'utilizzo di dati biometrici e sono proprio gli italiani tra i più favorevoli all'utilizzo della biometria per l'autenticazione nelle operazioni di pagamento. È quanto emerge da una ricerca effettuata in Europa da Visa. In particolare, gli europei sono convinti dell'efficacia di un sistema di autenticazione a due fattori, di cui uno basato sul controllo di un elemento biometrico, come la scansione dell'iride o dell'impronta digitale. Ciò vale per circa tre quarti della popolazione europea (73%) e poco più degli italiani (76%).

L'autenticazione a due fattori (ricordarlo non fa mai male) implica un qualcosa che si ha, come una carta o un telefonino e un qualcosa che si sa, come un PIN o una password. In sostituzione di questi ultimi si può usare un qualcosa di univocamente personale, come un parametro biometrico.

Utilizzando quest'ultimo il livello di sicurezza s'innalza, ovviamente, essendo più facile carpire una password o un pin, soprattutto per un cyber criminale che opera online, piuttosto che tranciare un dito per usarne l'impronta digitale e aprire una serratura biometrica, come immaginano fiction truculente.

Ma la sicurezza è certamente maggiore se la scansione del dato biometrico viene effettuata dal vivo, cioè alla presenza di un controllore, come può essere la cassiera di un supermercato. Se l'autenticazione avviene online, occorre ricordare che anche il dato biometrico è un dato digitale: la differenza, qui, la fa il metodo di input.



Gli italiani sopra la media europea

Queste considerazioni, tornando alla ricerca, non sembrano preoccupare i consumatori europei. Costoro, infatti, si fidano di un sistema a due fattori con parametro biometrico utilizzato in combinazione a un dispositivo fisico per l'autenticazione nel momento del pagamento, ma desiderano usare soluzioni biometriche per l'autenticazione anche sui siti di e-commerce.

La ricerca della semplicità e il bisogno di sicurezza

La chiave di questa scelta sta nel desiderio di trovare equilibrio tra sicurezza e facilità dei processi d'acquisto: il 67% dei consumatori riconosce l'importanza di soluzioni con caratteristiche che proteggano la propria identità. È auspicabile dunque che le nuove forme di autenticazione debbano raggiungere un equilibrio tra velocità dell'operazione e sicurezza. La ricerca ha rilevato, infatti, che l'autenticazione biometrica è considerata importante in egual misura sia negli acquisti face-to-face, quando cioè efficienza e velocità sono prioritarie, sia nelle transazioni online.

La quota di consumatori propensi alle tecnologie di biometria sale al 74% in Italia, la più alta registrata in Europa.

Jonathan Vaux, Executive Director Innovation Partnership di Visa, commenta: «L'identificazione e la convalida con parametri biometrici offre l'opportunità di semplificare e migliorare l'esperienza del cliente. La ricerca di Visa dimostra che la biometria

Biometrics per la semplicità

Alcuni dati emersi dalla ricerca:

- Il 48% vorrebbe usare l'autenticazione biometrica per i pagamenti sui trasporti pubblici
- Il 47% desidera utilizzare metodi di autenticazione biometrica per i pagamenti al bar o al ristorante
- Il 46% li utilizzerebbe per tutto lo shopping, dalla spesa quotidiana al caffè ai pagamenti al fast food
- Il 40% vorrebbe utilizzarlo per l'e-commerce
- Il 39% per pagare contenuti scaricati online

è riconosciuta come forma di autenticazione affidabile quanto più i consumatori prendono confidenza con l'utilizzo di queste funzionalità sui dispositivi in loro possesso».

La soddisfazione in Visa, riflette il punto di vista degli esercenti online, che possono cogliere un'opportunità, considerando, come ricordano gli autori della ricerca, che 31% dei consumatori ha abbandonato l'acquisto online a causa del processo di sicurezza del pagamento.

Al momento, però, i sistemi biometrici devono ancora superare la sfida negli scenari in cui è l'unica forma di autenticazione utilizzata. «Se usati come unico sistema di riconoscimento i dati biometrici possono risultare come un "falso positivo" o un "falso negativo" poiché, a differenza del PIN, codice numerico che può essere digitato in maniera corretta o sbagliata, non c'è una verifica binaria 'corretto/sbagliato', l'autenticazione biometrica, infatti, si basa sulle probabilità di corrispondenza tra i parametri inseriti», spiega Vaux, che aggiunge: «I sistemi biometrici di riconoscimento funzionano dunque al meglio se combinati con altri fattori quali il dispositivo fisico, le tecnologie di geo-localizzazione e metodi di autenticazione aggiuntivi. Visa ritiene



Metodologia della ricerca Populus

Visa ha commissionato l'indagine "Biometrics Payments" a Populus. Condotta tra il 22/04 e 6/05/2016, la ricerca è stata effettuata in 7 Paesi europei: Regno Unito, Svezia, Francia, Germania, Italia, Portogallo e Polonia. Il totale del campione è di 14.236 rispondenti, circa 2.000 per Paese (2035 il campione per l'Italia)

fondamentale quindi l'adozione di un approccio olistico che tenga conto dell'ampia gamma di tecnologie a sostegno del processo di autenticazione».

Se si prendono in considerazione i vantaggi dell'autenticazione biometrica, il 51% dei consumatori europei (57% degli italiani) è convinto che l'autenticazione biometrica nei pagamenti darà inizio a un'esperienza di pagamento più veloce e facile dei metodi tradizionali di pagamento.

Un terzo della popolazione europea (33% contro una media del 41% in l'Italia), invece, menziona, tra i benefici, la sicurezza dei dati che l'autenticazione biometrica garantisce anche in caso di furto o smarrimento del dispositivo di pagamento.

Sempre Vaux argomenta: «In futuro i consumatori avranno a disposizione un ventaglio sempre più ampio di scelte di modalità di pagamento. Come il modo di pagare cambia a seconda di dove ci si trova e da quale dispositivo si stia facendo shopping, così i metodi di autenticazione dovranno essere appropriati per ogni caso specifico».

Questo significa una continua evoluzione e apre a uno scenario ibrido: «Se le forme di autenticazione biometrica offrono l'opportunità di trovare una mediazione tra comodità e sicurezza non costituiscono

l'unica soluzione possibile. In futuro, utilizzeremo un mix di diverse soluzioni di autenticazione a seconda della situazione di acquisto. Abituandoci a riconoscere queste tecnologie come una forma valida di autenticazione oggi, saremo in grado di supportare l'ecosistema dei pagamenti nella sua fase di sviluppo in direzione della sicurezza, della praticità e dell'usabilità», conclude Vaux.

La popolarità delle impronte digitali - La ricerca, con uno studio condotto su oltre 14mila consumatori europei, rivela che la familiarità e la conoscenza delle forme di biometria sono fattori fondamentali per il progresso in questa direzione. Con il sopraggiungere dei pagamenti tramite dispositivi mobili, il riconoscimento delle impronte digitali sembra essere il metodo biometrico più promettente per la sua facilità di utilizzo e la sicurezza. Se si prende in considerazione esclusivamente la sicurezza percepita delle tecnologie biometriche, l'81% dei consumatori vede le impronte digitali come il parametro più affidabile, seguito dal riconoscimento dell'iride (76%). Ecco perché oltre la metà dei consumatori (53%) dichiara di prediligere le impronte digitali agli altri metodi di riconoscimento biometrico per i pagamenti.

BIOMETRIA E LEGGE: ISTRUZIONI PER L'USO

Le opportunità fornite dalle nuove tecnologie vanno adeguate al contesto e ben valutate, per non eccedere rischiando di violare il codice sulla privacy

di Riccardo Abeti, avv. partner ExpLegal

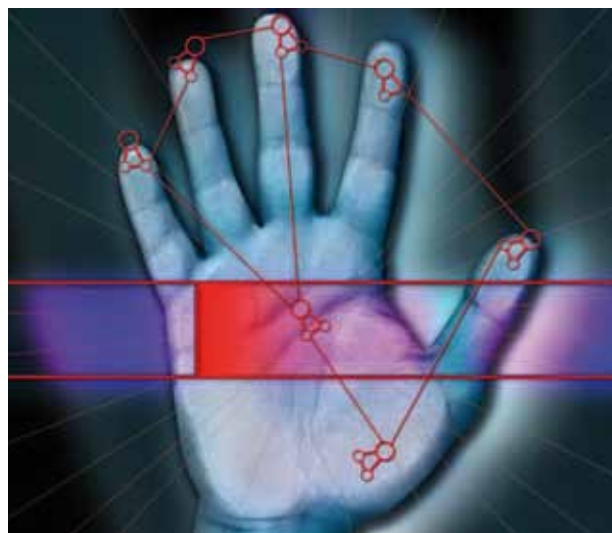
Nel tempo si susseguono e si inseguono molte mode, alcune parole chiave e alcuni concetti che sono considerati sinonimo di novità, di miglioramento, di incremento della sicurezza. Tra questi concetti alberga a buon diritto anche la "biometria". Oggi un lettore biometrico è sinonimo di maggior sicurezza, di avvenirismo e progresso.

Come sempre, occorre capire qual è l'oggetto della tutela a cui presidio poniamo un sistema biometrico e sulla base della risposta a questa domanda, pensare se effettivamente la biometria rappresenti una soluzione e a quali condizioni.

Molte realtà, non solo in ambito privato ma anche pubblico, stanno valutando la possibilità di adottare soluzioni di tipo biometrico.

Cosa occorre fare per realizzare un sistema che sia efficiente (ovvero che consenta di perseguire le finalità per le quali i dati sono stati raccolti), ma anche necessario (ossia non mero frutto di suggestioni ma il risultato di un'adeguata ponderazione)?

Per dotarci di un sistema biometrico, dobbiamo innanzitutto chiederci quale finalità perseguiamo,



perché questa ha un'intima connessione con gli strumenti e le metodologie utilizzate per soddisfarla. A seconda della finalità, la tecnologia biometrica può avere dei "propulsori" come: il marketing, la maggior sicurezza, la maggior praticità per gli utenti.

Poi occorre porsi un'altra domanda: le realtà del medesimo segmento quali tecnologie utilizzano?

La risposta a questa domanda porterà con sé due tipi di indicazioni:

1. la prima è relativa alla compliance con quanto indicato nel d.lgs. 30 giugno 2003, n. 196 (Codice privacy), in particolare con l'articolo 31;
2. la seconda aiuterà a focalizzare se la misura biometrica rappresenterà una tecnologia adeguata o d'avanguardia, oppure una tecnologia eccedente rispetto a quelle utilizzate dagli altri attori del medesimo segmento/categoria.



Per esempio, se per l'ingresso in una palestra gli operatori del settore utilizzano smartcard, strumenti NFC (Near Field Communication) o PIN, l'adozione di misure come l'analisi della "struttura vascolare della retina", può essere non solo economicamente dispendiosa (per quanto questa valutazione ricade esclusivamente nella pertinenza di chi conduce la valutazione), ma anche eccedente per perseguire la finalità di accesso alle strutture della palestra (omettere questa valutazione rischia di rendere il trattamento in contrasto con il Codice privacy).

Vi è poi una terza domanda, che tra l'altro incide notevolmente anche su questioni di profilo più pratico: quali norme regolamentano l'uso di questi strumenti?

Il codice della Privacy e il Provvedimento per i dati biometrici

Si parte dal Codice privacy, passando per lo specifico Provvedimento (e le allegate Linee guida) risalente al 2014, per finire con alcuni provvedimenti da quest'ultimo richiamati o più recenti. Gli articoli del Codice privacy, di particolare rilevanza in questo caso, sono i seguenti: 13, 17, 37, comma 1, lett. a), e 38.

Chi utilizza tecnologie con impatto sulla protezione dei dati e, più in generale, chi tratta dati personali, è avvezzo alla predisposizione dell'informativa per gli interessati (art. 13 del Codice privacy). Tuttavia in questo caso parliamo di alcuni dettagli di non secondaria importanza:

- L'informativa andrà resa prima dell'inizio del trattamento e il titolare dovrà fare esplicito riferimento all'utilizzo dei dati biometrici.
- Tra le modalità del trattamento enumerate nell'informativa occorrerà fare riferimento alle cautele adottate, ai tempi di conservazione dei dati e alla loro centralizzazione oppure alla loro esclusiva presenza su un dispositivo nell'esclusiva disponibilità dell'interessato.
- Occorrerà poi prevedere un sistema alternativo a quello biometrico laddove gli interessati non vogliano o non possano, anche in ragione di proprie caratteristiche fisiche, servirsi del sistema di riconoscimento biometrico.
- Nel caso in cui il dato biometrico sia registrato in un dispositivo posto nell'esclusiva disponibilità dell'interessato, l'informativa dovrà essere corredata di istruzioni per la corretta custodia e

sul “da farsi” in caso di smarrimento, sottrazione, malfunzionamento del dispositivo.

Inoltre, l’utilizzo di sistemi biometrici rientra tra i trattamenti che presentano rischi specifici di cui all’articolo 17 del Codice privacy e richiederà la c.d. “verifica preliminare” (che deve essere richiesta anteriormente all’inizio del trattamento) del Garante per la protezione dei dati personali.

Con la verifica preliminare l’Autorità potrà prescrivere, se necessario, misure e accorgimenti specifici per consentire il corretto utilizzo di dati così delicati nel contesto del trattamento prospettato.

Nell’istanza di verifica preliminare il titolare dovrà fornire diverse informazioni riguardanti l’analisi dei rischi condotta e le modalità con cui intende garantire il rispetto degli adempimenti giuridici e delle misure previste dallo specifico Provvedimento del Garante.

L’articolo 37, comma 1, lettera a), indica la necessità, nel caso in cui il trattamento riguardi dati biometrici, di procedere alla notificazione del trattamento secondo le modalità di cui all’articolo 38.

L'esenzione dalla notificazione

Dall’entrata in vigore del Codice privacy, il Garante ha adottato alcuni provvedimenti che hanno esentato dalla notificazione alcune categorie ovvero i titolari che perseguono determinate finalità.

Questi pronunciamenti del Garante sono:

- il provvedimento relativo ai casi da sottrarre all’obbligo di notificazione, 31 marzo 2004 (in G.U. n. 81 del 6 aprile 2004, doc. web n. 85261);
- il provvedimento recante “Chiarimenti sui trattamenti da notificare al Garante” 23 aprile 2004 (doc. web n. 993385) ed
- il provvedimento riguardante le “Notificazioni in



ambito sanitario: precisazioni del Garante” 26 aprile 2004 (doc. web n. 996680).

Il provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 (qui definito anche “Provvedimento”) è importante perché prevede indicazioni che riguardano la notificazione del trattamento e la verifica preliminare, nonché misure specifiche e l’introduzione della misura della data breach notification (corredata di apposita scheda per la segnalazione al Garante da parte del titolare del trattamento).

Come purtroppo avviene molto spesso, la parte meno intellegibile del Provvedimento è quella che riguarda l’esonero da questo o da quell’adempimento.

Nel caso di specie, l’esonero riguarda la verifica preliminare. Nel merito, le indicazioni sia per la superficialità con cui sono state lette dagli operatori del settore, sia, forse, per la genericità con cui sono state scritte, sono spesso state oggetto di fraintendimento da parte dei titolari del trattamento.

In sostanza, dalla lettura del Provvedimento e dei provvedimenti successivi a quello di cui stiamo trattando, se ne desume che le “aree sensibili” non



siano mai “il luogo di lavoro” nella sua interezza, ma solamente i luoghi ove sia richiesto un livello “ulteriore” di sicurezza oppure luoghi all’interno dei quali si registri la presenza di apparati e macchinari pericolosi.

Dati biometrici solo se necessari?

Con provvedimento del dicembre 2015 e con successivo provvedimento del marzo 2016, l’Autorità ha sottolineato quello che, allo stato attuale, è un principio dirimente nella scelta, da parte del titolare del trattamento, delle soluzioni di tipo biometrico: i dati biometrici possono essere raccolti e utilizzati solo in mancanza di una procedura equivalente e meno invasiva. Insomma, specie nel caso di rilevazione delle presenze dei lavoratori, i sistemi biometrici devono essere adottati solo in presenza di documentata inefficacia o impraticabilità di altri sistemi meno invasivi.

Per esempio nei casi dei cosiddetti “furbetti del cartellino” i precedenti sembrano giustificare la necessità di evitare continui “appostamenti” e verifiche, superando il problema con un sistema che

collochi, univocamente, il lavoratore laddove dovrebbe trovarsi al momento della registrazione del proprio accesso o del proprio allontanamento dagli uffici. Questa constatazione non comporta, tuttavia l’esonero dalla necessità di sottoporre il sistema adottato alla “verifica preliminare” del Garante.

È pur vero che in ambienti piccoli quella biometrica è la misura più agevole per evitare un’elevata, e spesso controproducente, percezione dei controlli sul personale.

Si pensi a un piccolo ente locale ove la verifica di un badge (se si stia utilizzando quello proprio o quello altrui), da parte di un collega a ciò preposto, viene vissuta quasi come una forma di mobbing (fatto vissuto in modo ben diverso nei grandi enti).

Conclusioni

In conclusione, l’uso della biometria può rappresentare un upgrade del livello di sicurezza di un sistema ma non deve far dimenticare che ha un notevole impatto in termini di regolamentazione; l’introduzione di un sistema biometrico va studiata attentamente perché non può essere considerata la panacea di tutti i mali.

Un sistema biometrico deve essere concepito nell’ambito di un sistema “sicuro” e non aggiunto come “toppa” per innalzare il livello di sicurezza (nella maggior parte dei casi “l’aggiunta posticcia” non genera i risultati attesi). In questo senso si esprime il Regolamento privacy (Regolamento (UE) 2016/679) - adottato dall’Unione Europea che sarà applicabile dal maggio 2018 – il quale prevede che le soluzioni che incidono sul trattamento dei dati personali, siano pensate ab initio in termini di sicurezza by default e privacy by design.

SECURITY TESTING CON IL NUOVO TEAM IBM X-FORCE RED

*Charles Henderson,
Global Head of Security
Testing and X-Force
Red di IBM*

Ibm amplia la propria squadra di esperti con l'ingresso di nuovi professionisti ed ethical hacker e continua a investire in consulenza e servizi per la sicurezza

di Gaetano Di Blasio



Si chiama X-Force Red, il nuovo team per il security testing, pensato per aiutare le imprese a identificare le vulnerabilità presenti nei propri sistemi hardware e software. Il nuovo gruppo di esperti è istituito all'interno degli Ibm Security Services e acquisisce, accanto ai professionisti già operativi nella business unit ulteriori talenti nella sicurezza di fama mondiale e hacker etici. X-Force Red controllerà le vulnerabilità di sicurezza legate al fattore umano e relative ai processi e alle procedure quotidiane.

Con il ruolo di Global Head of Security Testing and X-Force Red, sarà Charles Henderson di IBM, esperto ben noto nel campo dei penetration test, a coordinare un network della sicurezza. A supporto del team, la security intelligence di IBM X-Force Research, della piattaforma di condivisione delle minacce IBM X-Force Exchange e di IBM Security AppScan per fornire un ulteriore livello di sicurezza.

«Avere un mezzo di scansione automatica dei propri server e del codice sorgente è un notevole aiuto nella prevenzione delle violazioni dei dati, ma nei security testing non va trascurato l'elemento umano», sottolinea Henderson, che aggiunge: «I migliori esperti possono apprendere come funziona un ambiente e creare modalità uniche di attacco utilizzando

tecniche più sofisticate di quelle a disposizione dei criminali».

Quattro aree di focalizzazione

Le quattro aree di focalizzazione di IBM X-Force Red sono:

Applicazioni – penetration testing e revisione del codice sorgente per identificare le vulnerabilità di sicurezza nelle varie piattaforme (web, applicazioni mobili, terminali, mainframe e middleware).

Rete – penetration testing delle frequenze interne, esterne, wireless e delle frequenze radio di altro tipo.

Hardware – verifica della sicurezza tra gli ambienti fisici e digitali attraverso test dell'Internet of Things (IoT), dei dispositivi wearable, dei sistemi POS, dei bancomat, dei sistemi automotive e dei kiosk self-service.

Fattore umano – esecuzione di simulazioni di phishing, di social engineering, di ransomware e di violazioni della sicurezza fisica per determinare i rischi legati al comportamento umano

IBM X-Force Red fornisce servizi di security testing secondo tre modelli: singoli progetti, attività di test in abbonamento e programmi di testing gestiti



Gastone Nencini,
country
manager di
Trend Micro
Italia



La pubblicazione di informazioni, foto e video personali offre innumerevoli opportunità al cybercrime per violare la nostra privacy, sottrarre dati personali e causare danni economici. Poche semplici regole riducono molto i rischi

I social media sono un fenomeno che coinvolge stabilmente centinaia di milioni di utenti e, per questo, sono stabilmente al centro dell'interesse del cybercrime. La pubblicazione di informazioni personali liberamente accessibili mette a disposizione dei criminali informatici preziose indicazioni per sferrare attacchi efficaci, individuare password e svolgere altre azioni nocive.

Per esempio, un post su un agriturismo che avete visitato la domenica, può fornire lo spunto a un malintenzionato per comporre una e-mail contenente proposte di promozione, annunci di iniziative o foto legate a questo agriturismo aumentando enormemente le probabilità di farvi aprire la e-mail, cliccare su un link che vi indirizza verso un sito fraudolento o farvi scaricare un allegato contenente un malware. La sottrazione di informazioni personali è anche alla base del furto d'identità, uno dei pericoli più frequenti in cui possono incorrere gli utenti dei social network (e non solo). L'obiettivo è di accedere a dati personali e sensibili per poi rivenderli al mercato nero (incredibilmente florido).

I social network e lo scambio di messaggi che li contraddistinguono stanno diventando anche un veicolo importante per la distribuzione di malware.

Conoscere i possibili rischi permette di utilizzare i social network in modo più responsabile e sicuro. e poche semplici regole possono già ridurre di molto le insidie in agguato dietro l'angolo.

Innanzitutto, è opportuno non aprire e-mail provenienti da mittenti sconosciuti o sospetti ed evitare di accedere a Url, anche nel caso di rimandi a siti apparentemente noti, cliccando sui link presenti all'interno della e-mail. Ricordate che anche all'interno di semplici fotografie possono essere inseriti codici in grado di compromettere il vostro pc. Ancora più cautela va posta nello scriccare allegati.

È anche opportuno fare attenzione alle impostazioni predefinite dei social network, fornendo in modo consapevole le autorizzazioni di accesso alle informazioni private solo alle persone conosciute e verificate. Spesso, infatti, gli amici on-line non si conoscono nella vita reale ed è molto facile apparire per ciò che non si è, perché i siti, normalmente, non verificano la veridicità dell'identità di chi crea un account. Peraltro anche la sicurezza fisica risente dei rischi legati ai social network: nel periodo estivo postare foto da un lontano atollo dei Caraibi significa informare i ladri di appartamento che non sarete a casa per un po' di tempo.



IDC DIGITAL TRANSFORMATION CONFERENCE 2016

Staying Ahead of the Innovation Curve

29 Settembre | Milano, Centro Svizzero

Scenario

Le tecnologie e i processi di un'azienda sono ormai così strettamente legati ai clienti e ai mercati che i confini tra le operazioni interne e l'ecosistema esterno (i clienti appunto ma anche i partner, i concorrenti, i regolatori) stanno rapidamente scomparendo. Per crescere e competere in un mondo sempre più digitale, le aziende dovranno pertanto trasformare e innovare con tecnologie digitali i modelli organizzativi, operazionali e di business. Data la dipendenza di questo processo dall'IT e dalle informazioni aziendali, il CIO giocherà un ruolo importante a fianco e per il business. IDC ritiene che il successo di una trasformazione digitale molto dipenderà infatti dal grado di integrazione, elasticità e sicurezza che l'IT garantirà. Al CIO si chiederà non solo di colmare il gap tra IT e digitale, ma anche un forte ruolo di governance e di innovazione per mantenere allineati i servizi IT alla velocità dei mercati.

Key Words

Digital transformation, Customer experience, Customer experience IT (CXIT), CIO/CMO collaboration, IT purchases & funding, Business digitalization, Omnichannel, Cloud, Mobile, Social, Big data, Analytics, IoT.

Premium
Sponsor

COMMVault 

HITACHI 
Inspire the Next

Main
Sponsor



servicenow

PER INFORMAZIONI

Nicoletta Puglisi, Senior Conference Manager, IDC Italia
npuglisi@idc.com · 02 28457317

http://www.idcitalia.com/ita_DX16

 #IDCDX16

 **IDC**
Analyze the Future

