Da ricerche Immuniweb sulla sicurezza: il 64% delle aziende fintech non supera il test Gdpr

Internet banking, si apre una falla

L'obiettivo della sicurezza privacy online è ancora lontano. Tecnofinanza e banche online non superano il test della privacy europea, e cioè l'esame di conformità al Regolamento generale Ue 2016/679 sulla protezione dei dati (noto anche come Gdpr).

Due ricerche di Immuniweb passano ai raggi X la sicurezza delle imprese bancarie e del mondo del fintech e i dati rivelano un quadro di forti criticità. Nel settore della tecnofinanza, il 64% delle aziende fintech ha fallito il test di conformità al Gdpr per il proprio sito Web principale. Il 100% delle banche presenta vulnerabilità di sicurezza o problemi relativi a sottodomini dimenticati.

Quanto al settore bancario il 97% delle più grandi banche è a rischio di furto di dati online, e il 20% delle app di mobile banking contiene almeno una vulnerabilità di sicurezza ad alto rischio. Inoltre di 100 banche esaminate, 85 app di web banking non superano il test di conformità al Gdpr, 25 non sono protette da firewall, e 7 contengono vulnerabilità note e sfruttabili dagli hacker.

Beninteso, il settore creditizio e finanziario non è l'unico a mostrare problemi di conformità al Gdpr. Altre indagini, per esempio, hanno svelato che ad arrancare è anche il settore delle pubbliche amministrazioni: una ricerca della Global Privacy Enforcement Network (Gpen) per il 2018 risulta che il 48% delle Regioni non ha policy e procedure per la gestione di richieste e reclami da parte degli interessati; il 20% delle regioni non ha ancora adottato una procedura interna per la gestione dei dati; addirittura il 58% non ha processi documentati per la valutazione di impatto. Inoltre un quinto delle organizzazioni non ha ancora una procedura di risposta agli incidenti di sicurezza (data breach) e un quarto non ha nemmeno un registro per documentare le violazioni subite. Il 58% delle regioni (e il 24% delle società in-house) non ha processi per la valutazione dei rischi sulla protezione dei dati personali, in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi.

Tornando al settore creditizio, la ricerca Immuniweb (reperibile integralmente all'indirizzo https://www.immuniweb.com/blog/SP-100-banks-application-security.html), diffusa da Federprivacy, ha valutato il grado di adeguamento privacy alla normativa europea in relazione ai principi del trattamento e responsabilizzazione (articolo 5 Gdpr), consenso e altre condizioni di liceità (articolo 6 e 7), privacy by design (articolo 25), misure di sicurezza (articolo 32) e valutazione di impatto privacy (articolo 35).

In questo settore è emerso anche che, quanto alla conformità a standard normativi e tecnici, 85 applicazioni web e-banking non hanno superato il test di conformità al Gdpr, 49 applicazioni web di e-banking non hanno superato il test di conformità PCI DSS, 25 applicazioni Web di e-banking non sono protette da un Web Application Firewall.

Sempre nel settore bancario, ma in relazione ai parametri di vulnerabilità di sicurezza, la ricerca Immuniweb attesta che 7 applicazioni web di e-banking contengono vulnerabilità note e sfruttabili, il 92% delle applicazioni di mobile banking contiene almeno una vulnerabilità di sicurezza a medio rischio e il 100% delle banche presenta vulnerabilità di sicurezza o problemi relativi a sottodomini dimenticati.

Nel settore fintech (https://www.immuniweb.com/blog/fintech-application-security.html), Immuniweb testimonia che il 100% delle aziende ha problemi di sicurezza, privacy e conformità relativi ad applicazioni Web, API e sottodomini abbandonati o dimenticati, mentre 8 siti Web principali e 64 sottodomini delle società hanno almeno una vulnerabilità di sicurezza divulgata pubblicamente e sfruttabile a medio o alto rischio.

Inoltre il 100% delle applicazioni mobili contiene almeno 1 vulnerabilità di sicurezza a rischio medio, il 97% presenta almeno 2 vulnerabilità a rischio medio o alto. Il 56% dei back-end di app mobili (API REST / SOAP) presenta gravi configurazioni errate o problemi di privacy relativi alla configurazione SSL / TLS e insufficiente protezione della sicurezza del server Web.

In materia di conformità il 62% delle aziende fintech passate al setaccio ha fallito il test di conformità PCI DSS anche per il proprio sito web principale e il 64% delle aziende ha fallito il test di conformità al Gdpr sempre per il proprio sito web principale.

La considerazione che si trae da questo quadro è che è necessario rafforzare la fiducia degli utenti dei servizi della società dell'informazione a qualunque settore appartengono, imprenditoriale o delle pubbliche amministrazioni e, soprattutto, rendere riconoscibili i soggetti meritevoli di affidamento.

A tale riguardo ci sono esperienze in corso sviluppate all'interno di un contesto volontario e di regolamentazione sotto la supervisione di soggetti riconosciuti.

Un esempio è il marchio Il marchio «Privacy Ok» per i siti internet, varato da Federprivacy, rilasciato ad aziende ed enti che aderiscono a uno specifico codice di condotta. L'associazione informa che sono oltre trenta i siti e le app di banche e istituti di credito che hanno richiesto il marchio «Privacy Ok». Federprivacy ha affidato il processo di valutazione a TÜV Italia, organismo di certificazione indipendente, che assicura l'imparzialità del processo per determinare se un sito è effettivamente conforme per la concessione del marchio.

Altre opzioni potranno derivare dal Gdpr e dalla futura normativa in materia di certificazioni (articolo 42 Gdpr).

I dati per le banche

Conformità	85 applicazioni web e-banking non conformi al Gdpr
	49 applicazioni web di e-banking non conformi al PCI DSS
	25 applicazioni Web di e-banking non protette da un Web Application Firewall
Vulnerabilità di sicurezza	7 applicazioni web di e-banking contengono vulnerabilità note e sfruttabili
	92% delle app di mobile banking con almeno 1 vulnerabilità di sicurezza a medio rischio
	100% delle banche con vulnerabilità di sicurezza o problemi relativi a sottodomini dimenticati

Fonte: https://www.immuniweb.com/blog/SP-100-banks-application-security.html

L'omessa notifica degli incidenti può costare fino a 10 milioni di euro

L'omessa notifica del data breach al Garante può costare cara: si applica la sanzione fino a 10 milioni di euro o fino al 2% del fatturato. Il regolamento Ue sulla protezione dei dati 2016/679 (Gdpr) dimostra anche nelle disposizioni sanzionatorie quanto sia importante gestire al meglio una violazione della sicurezza che danneggi i dati personali. Il Garante della privacy ha elaborato un vademecum, nel quale riepiloga modalità e termini degli adempimenti in capo a imprese ed enti nel caso di una violazione della sicurezza (data breach).

Definizione di data breach. **Il data breach è una violazione di sicurezza che comporta, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. La violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.**

Adempimenti. **In caso di violazione dei dati personali, il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista) senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, deve effettuare due adempimenti: 1) notificare la violazione al Garante a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche; 2) comunicare l'accaduto agli interessati.**

Il responsabile del trattamento (per esempio un fornitore esterno di servizi) che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurne l'impatto.

Registro delle violazioni. **Il titolare del trattamento, a prescindere dalla notifica al Garante, deve documentare tutte le violazioni dei dati personali, per esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.**

Oggetto. **Il Garante ha precisato che vanno notificate unicamente le violazioni di dati personali che possono avere effetti avversi significativi sugli individui, causando danni fisici, materiali o immateriali.**

Ciò può includere, per esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

Modalità. **La notifica deve contenere le informazioni previste all'articolo 33, par. 3 del Regolamento (UE) 2016/679 e indicate nel Provvedimento del Garante del 30 luglio 2019.**

Se si utilizza per la notifica il modello allegato al provvedimento, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

La notifica deve essere inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) oppure con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura «notifica violazione dati personali» e opzionalmente la denominazione del titolare del trattamento.

Sanzioni. **Il Garante può prescrivere misure correttive nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato totale annuo mondiale.**