Grande fermento normativo sui temi di sicurezza informatica e gestione dei rischi!

Il percorso di **Digital Transformation**, oltre alla valutazione di nuove **opportunità** di **business** e di **relazione** con la **clientela**, è accompagnato dalla crescente attenzione del **legislatore**, nazionale ed europeo, verso i temi di **sicurezza informatica**, con l'obiettivo di garantire un'adeguata gestione dei dati e dei servizi digitali offerti all'utente.

Dal **2013** si è assistito a una **proliferazione di norme e raccomandazioni in materia**, con un impatto per le **banche** italiane:

PAGAMENTI

Raccomandazioni BCE sulla sicurezza dei pagamenti Internet ✓

Orientamenti EBA sulla sicurezza dei pagamenti Internet ✓

Nuova Payment Service Directive (PSD2) ✓

RTS EBA su strong authentication e relazione con le TP ⚠

RISCHIO INFORMATICO, INCIDENTI E SICUREZZA DI INFORMAZIONI E RETI

Disposizioni di Vigilanza Prudenziale di Banca d'Italia (circolare 285) ✓

Direttiva NIS ⚠

PROTEZIONE DEI DATI , TRATTAMENTO E CIRCOLAZIONE DI INFORMAZIONI

Circolazione delle informazioni bancarie e il trattamento dei dati bancari (Garante II) ✓

General Data Protection Regulation (GDPR) ✓

✓ emanato ⚠ in corso di emanazione

Sicurezza dei pagamenti Internet

RACCOMANDAZIONI BCE - SECURE PAY

- Le **Disposizioni di Vigilanza recepiscono le Raccomandazioni SecuRePay**, indicando una serie di indicazioni e best practice cui le banche si sono dovute adeguare entro il 1° febbraio 2015, salvo scegliere approcci differenti giustificati da adeguate analisi del rischio (***comply or explain***)

ORIENTAMENTI EBA

- Pubblicati a dicembre 2014, riprendono i contenuti delle **Raccomandazioni SecuRePay** sulla sicurezza dei pagamenti internet, rafforzandone **la base legale**.
- Con gli **Orientamenti EBA viene meno** il principio del ***comply or explain*** e si ripropongono le **Migliori Prassi** che i **prestatori** di **servizi di pagamento** e gli **operatori di mercato sono invitati a valutare**
- Secondo quanto previsto dai principi guida degli Orientamenti, le attività previste sono:

Recepiti nell'ordinamento di Banca d'Italia con il 16° aggiornamento della Circolare 285 di Banca d'Italia

- Realizzazione di un **assessment specifico** dei **rischi** connessi all'offerta dei servizi di pagamento on line (fornite indicazioni di carattere organizzativo e operativo);
- Introduzione di **strong authentication** per l'inoltro dei pagamenti via Internet e per l'accesso ai dati sensibili di pagamento;
- Implementazione di **procedure efficaci** in merito all'autorizzazione e monitoraggio delle transazioni per identificare comportamenti anomali e prevenire le frodi;
- Promozione di **iniziative di sensibilizzazione** della **clientela**.

Recepimento degli Orientamenti EBA nell'ordinamento italiano

Il **16° aggiornamento** del **17 maggio 2016** della **Circolare 285 recepisce nell'ordinamento italiano** gli **Orientamenti EBA** sulla sicurezza dei pagamenti tramite internet, **sostituendosi** alle **Raccomandazioni BCE**

- È introdotta nel Titolo IV, Capitolo 4 «Sistemi informativi» una specifica **Sezione VII** che disciplina gli aspetti **sicurezza dei pagamenti via Internet**, rimandando agli Orientamenti
- **Gli Orientamenti sono recepiti in maniera integrale** mentre le **Migliori Prassi** sono **facoltative** e rimandate alla valutazione delle singole banche.

Le banche si adeguano agli obblighi imposti entro il 30 settembre 2016

«Le banche applicano le disposizioni contenute negli Orientamenti secondo il principio di proporzionalità, cioè tenuto conto della dimensione e complessità operative, della natura dell'attività svolta, della tipologia dei servizi prestati.»

- Entro il **30 ottobre 2016** le banche **trasmettono** alla **Banca Centrale Europea o** alla **Banca d'Italia** una **relazione**, approvata dall'organo con funzione di supervisione strategica, sugli **interventi effettuati** sulla struttura organizzativa e di controllo nonché sui sistemi informativi al fine di assicurare il rispetto degli obblighi introdotti con il presente aggiornamento.

Orientamenti EBA su sicurezza pagamenti Internet

Contenuti

CONTROLLO GENERALE E AMBIENTE DI SICUREZZA

1. Governance (policy)
2. Valutazione dei rischi
3. Monitoraggio e segnalazione degli incidenti
4. Controllo e mitigazione dei rischi
5. Tracciabilità

MISURE SPECIFICHE DI CONTROLLO E DI SICUREZZA PER I PAGAMENTI VIA INTERNET

6. Identificazione iniziale dei clienti, informazioni
7. Autenticazione forte del cliente
8. Iscrizione (enrolment) e fornitura di strumenti e/o software di autenticazione al cliente
9. Tentativi di accesso, sessione scaduta, validità di autenticazione
10. Monitoraggio delle operazioni
11. Protezione dei dati sensibili relativi ai pagamenti

SENSIBILIZZAZIONE, EDUCAZIONE E COMUNICAZIONE RIGUARDANTI IL CLIENTE

12. Educazione e comunicazione riguardanti il cliente
13. Comunicazioni, fissazione di limiti
14. Accesso dei clienti alle informazioni sullo stato dell'ordine e sull'esecuzione dei pagamenti

Allegato – Migliori Prassi

Fonte: EBA – Guidelines on the security of internet payments, 2015 - http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

Orientamenti EBA su sicurezza pagamenti Internet

Focus autenticazione forte del cliente

ABI Lab
Tecnologia utile

IL RICORSO ALLA STRONG AUTHENTICATION

*L'inoltro dei **pagamenti via Internet**, così come l'**accesso ai dati sensibili** relativi ai pagamenti, **dovrebbero essere protetti da un'autenticazione forte del cliente**. […]*

***Autenticazione forte del cliente** è, ai fini dei presenti orientamenti, una **procedura basata sull'impiego di due o più dei seguenti elementi** - classificati nelle categorie della conoscenza, del possesso e dell'inerenza: **i) qualcosa che solo l'utente conosce**, per esempio una password statica, un codice, un numero di identificazione personale; **ii) qualcosa che solo l'utente possiede**, per esempio un token, una smart card, un cellulare; **iii) qualcosa che caratterizza l'utente**, per esempio una caratteristica biometrica, quale può essere un'impronta digitale. Inoltre, **gli elementi selezionati devono essere reciprocamente indipendenti**, ossia la violazione di un elemento non compromette l'altro o gli altri. **Almeno uno degli elementi dovrebbe essere non riutilizzabile e non replicabile** (eccettuata la categoria dell'inerenza) e non atto a essere indebitamente carpito via Internet. La procedura di autenticazione forte dovrebbe essere concepita in modo tale da proteggere la riservatezza dei dati di autenticazione*

- Uno degli elementi su cui è necessario puntare l'attenzione riguarda la **definizione** adottata di "***strong authentication***" che include anche i requisiti di ***non-reusabilità*** **e** ***non replicabilità*** di almeno uno dei mezzi utilizzati → **REQUISITI NON PRESENTI NELLA PSD2!**

- Nell'Orientamento 7 sono stati al contempo elencati **esplicitamente** i casi in cui i **PSP** possono adottare **misure alternative di autenticazione** della clientela:
  - **pagamenti verso beneficiari sicuri, precedentemente inseriti in apposite white list;**
  - **transazioni tra due account dello stesso cliente presso lo stesso PSP;**
  - **trasferimenti all'interno dello stesso PSP giustificati dalla risk analysis;**
  - **pagamenti di importi ridotti, come previsto nella PSD**.

Fonte: EBA – Guidelines on the security of internet payments, 2015 - http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

Le tecnologie in uso presso le banche

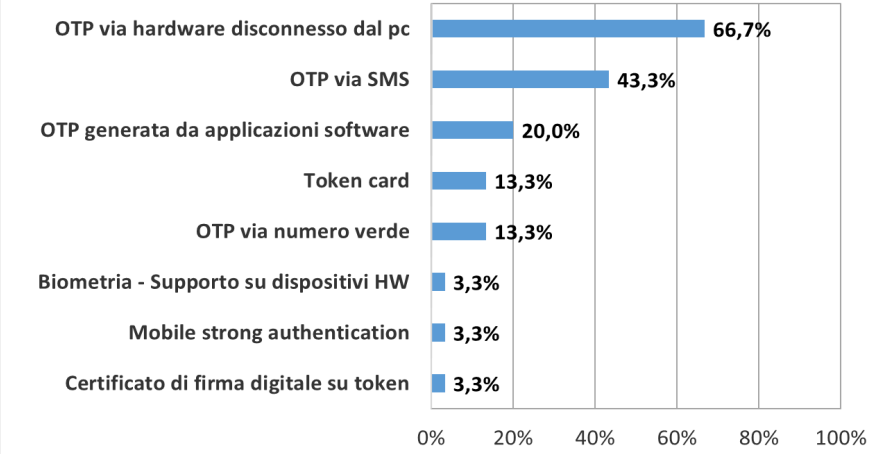
Strumenti di autenticazione forte per il cliente

ABI Lab
Tecnologia utile

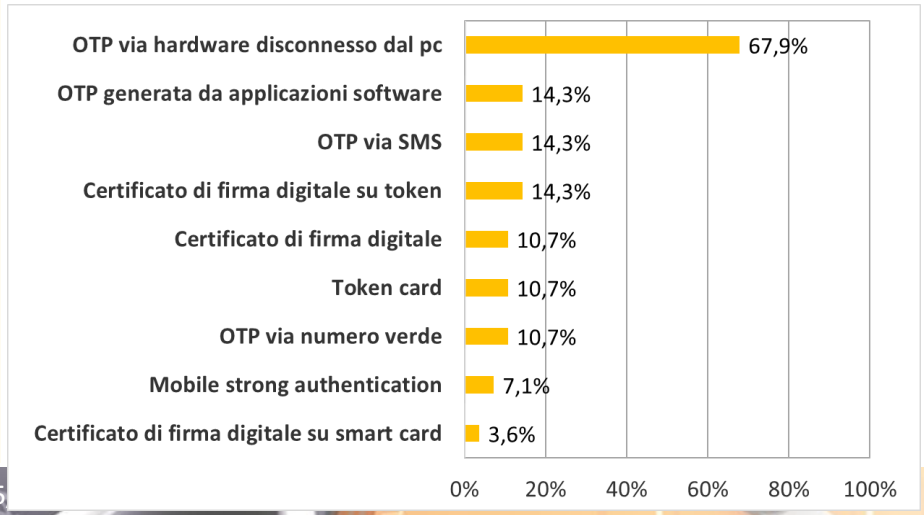
La totalità delle banche mette a disposizione tecnologie di strong authentication

Secondo fattore di autenticazione – Diffusione tecnologie (segmento Retail – 30 rispondenti)

- Il **50%** delle banche offre **due differenti tecnologie**, il 17% tre e il 3% quattro
- Le soluzioni maggiormente diffuse prevedono l'invio dell'**OTP su token o via SMS**
- **L'80%** del campione mette a disposizione un **canale alternativo** di comunicazione in fase di **notifica** delle operazioni (principalmente **SMS**)



Secondo fattore di autenticazione – Diffusione tecnologie (segmento Corporate – 28 rispondenti)



- Il 39% delle banche mette a disposizione due **differenti tecnologie**, il 14% tre
- Maggiore diffusione rispetto al segmento Retail di **soluzioni di firma digitale**
- **Canale alternativo** offerto in fase di **notifica** dal **64,3%** delle banche (principalmente **e-mail**)

Fonte: ABI Lab – Osservatorio Sicurezza e Frodi Informatiche – Rilevazione sulle frodi Internet e Mobile Banking, 2016

PSD2

Principali punti di attenzione sotto il profilo della sicurezza (1/5)

È stato pubblicato alla **fine del 2015** il nuovo testo della **PSD**, che presenta significative **novità** sotto il profilo della **sicurezza**, con particolare riferimento ai seguenti punti:

Definizioni chiave

- *Articolo 4 Definizioni*

Servizi offerti da TP / Diritti e obblighi / Autorizzazione ed esecuzione operazioni di pagamento

- *Articolo 45 Informazioni e condizioni*
- *Articolo 46 Informazioni per il pagatore e per il beneficiario dopo che l'ordine di pagamento è stato disposto*
- *Articolo 66 Disposizioni per l'accesso ai conti di pagamento in caso di servizi di disposizione di ordine di pagamento*
- *Articolo 67 Disposizioni per l'accesso alle informazioni sui conti di pagamento e all'utilizzo delle stesse in caso di servizi di informazione sui conti*
- *Articolo 68 Limiti dell'utilizzo degli strumenti di pagamento e dell'accesso ai conti di pagamento da parte dei prestatori di servizi di pagamento*
- *Articolo 69 Obblighi a carico dell'utente di servizi di pagamento in relazione agli strumenti di pagamento e alle credenziali di sicurezza personalizzate*

PSD2

Principali punti di attenzione sotto il profilo della sicurezza (2/5)

Servizi offerti da TP / Diritti e obblighi / Autorizzazione ed esecuzione operazioni di pagamento

- *Articolo 70 Obblighi a carico del prestatore di servizi di pagamento in relazione agli strumenti di pagamento*
- *Articolo 72 Prova di autenticazione ed esecuzione delle operazioni di pagamento*
- *Articolo 73 Responsabilità del prestatore di servizi di pagamento per le operazioni di pagamento non autorizzate*
- *Articolo 74 Responsabilità del pagatore per le operazioni di pagamento non autorizzate*
- *Articolo 89 Responsabilita dei prestatori di servizi di pagamento per la mancata esecuzione o l'esecuzione inesatta o tardiva delle operazioni di pagamento*

Data protection

- *Articolo 94 Protezione dei dati*

Rischi operativi e di sicurezza e procedure di autenticazione

- *Articolo 95 Gestione dei rischi operativi e di sicurezza*
- *Articolo 96 Notifica degli incidenti*
- *Articolo 97 Autenticazione*
- *Articolo 98 Norme tecniche di regolamentazione in materia di autenticazione e comunicazione*

PSD2

Principali punti di attenzione sotto il profilo della sicurezza (3/5)

- **DEFINIZIONI**

– Articolo 4 Definizioni

(15): 'servizio di disposizione di ordine di pagamento' un servizio che dispone l'ordine di pagamento su richiesta dell'utente di servizi di pagamento relativamente a un conto di pagamento detenuto presso un altro prestatore di servizi di pagamento;

(16): 'servizio di informazione sui conti' un servizio online che fornisce informazioni consolidate relativamente a uno o piu conti di pagamento detenuti dall'utente di servizi di pagamento presso un altro prestatore di servizi di pagamento o presso piu prestatori di servizi di pagamento;

«TERZE PARTI»

(18): 'prestatore di servizi di disposizione di ordine di pagamento' un prestatore di servizi di pagamento che esercita l'attivita di cui al punto 7 dell'allegato I (articolo 4 comma 15);

(19): 'prestatore di servizi di informazione sui conti' un prestatore di servizi di pagamento che esercita l'attivita di cui al punto 8 dell'allegato I (articolo 4 comma 16);

(29): 'autenticazione' la procedura che consente al prestatore di servizi di pagamento di verificare l'identità di un utente di servizi di pagamento o la validità dell'uso di uno specifico strumento di pagamento, compreso l'uso delle credenziali di sicurezza personalizzate dell'utente;

(30): 'autenticazione forte del cliente' un'autenticazione basata sull'uso di due o piu elementi, classificati nelle categorie della conoscenza (qualcosa che solo l'utente conosce), del possesso (qualcosa che solo l'utente possiede) e dell'inerenza (qualcosa che caratterizza l'utente), che sono indipendenti, in quanto la violazione di uno non compromette l'affidabilita degli altri, e che e concepita in modo tale da tutelare la riservatezza dei dati di autenticazione;

(31): 'credenziali di sicurezza personalizzate' funzionalita personalizzate fornite a un utente di servizi di pagamento dal prestatore di servizi di pagamento a fini di autenticazione;

• RISCHI OPERATIVI E DI SICUREZZA E PROCEDURE DI AUTENTICAZIONE (1/2)

– Articolo 97 Autenticazione

(1): Gli Stati membri provvedono a che un prestatore di servizi di pagamento applichi l'autenticazione forte del cliente quando il pagatore:

(a) accede al suo conto di pagamento on-line;

(b) dispone un'operazione di pagamento elettronico;

(c) effettua qualsiasi azione, tramite un canale a distanza, che puo comportare un rischio di frode nei pagamenti o altri abusi.

Ambiti di utilizzo dell'autenticazione forte del cliente

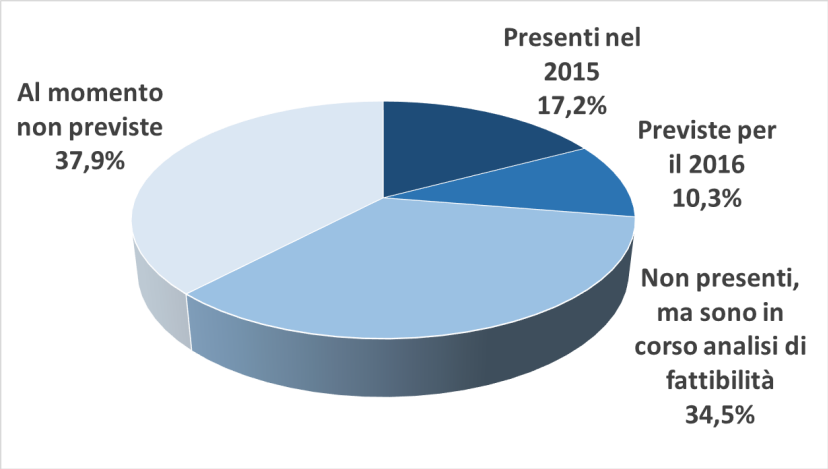
(2): Nel caso dell'avvio di un'operazione di pagamento elettronico a distanza i cui al paragrafo 1, lettera b), gli Stati membri provvedono affinche, per le operazioni di pagamento elettronico a distanza, i prestatori di servizi di pagamento applichino l'autenticazione forte del cliente che comprenda elementi che colleghino in maniera dinamica l'operazione a uno specifico importo e a un beneficiario specifico.

"Autenticazione forte" legata dinamicamente alla singola transazione, in particolare all'importo e al beneficiario.
A oggi considerata una Best Practice negli Orientamenti EBA sulla sicurezza dei pagamenti Internet

Tecnologie di autenticazione forte

Strong authentication legata dinamicamente a importo e beneficiario

Tecnologie di autenticazione forte legata dinamicamente alla singola transazione (segmento Retail, 29 rispondenti)

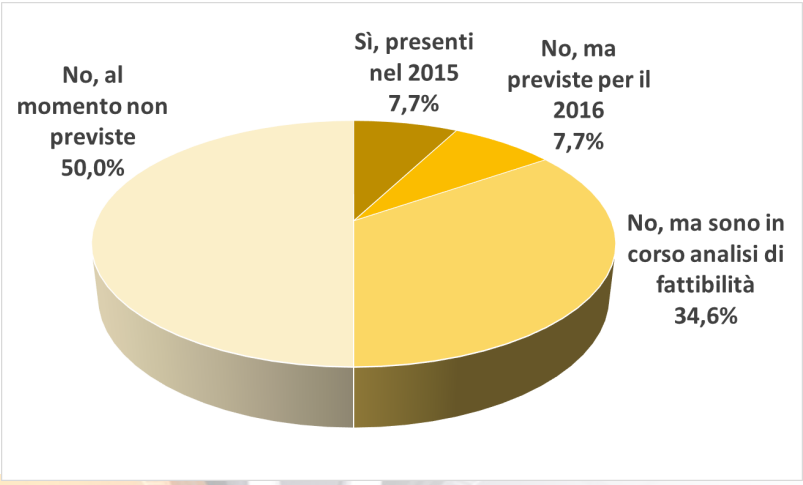


- Richieste dalla normativa a partire dalla fine del 2018, ma **in uso già in oltre il 17% delle banche**
- Più del **44%** delle banche ha **già identificato o sta valutando la tecnologia da adottare**

- **Oltre il 15%** del campione ha già identificato la **soluzione da adottare**
- Quasi il **35%** sta già svolgendo **analisi di fattibilità** per l'introduzione di queste tecnologie

In corso discussioni e confronti nei tavoli di lavoro per **identificare le soluzioni più idonee**

Tecnologie di autenticazione forte legata dinamicamente alla singola transazione (segmento Corporate, 26 rispondenti)



Fonte: ABI Lab – Osservatorio Sicurezza e Frodi Informatiche – Rilevazione sulle frodi Internet e Mobile Banking, 2016

• RISCHI OPERATIVI E DI SICUREZZA E PROCEDURE DI AUTENTICAZIONE (2/2)

– Articolo 98 Norme tecniche di regolamentazione in materia di autenticazione e comunicazione

(1): *In stretta **cooperazione** con la **BCE** e previa consultazione di tutti i portatori di interessi - anche quelli del mercato dei servizi di pagamento - tenendo conto di tutti gli interessi coinvolti, l'**EBA** emana, a norma dell'articolo 10 del regolamento (UE) n. 1093/2010, **progetti di norme tecniche di regolamentazione** indirizzati ai prestatori di servizi di pagamento, di cui all'articolo 1, paragrafo 1, della presente direttiva, in cui sono specificati:*

a) i requisiti dell' autenticazione forte del cliente *di cui all'articolo 97, paragrafi 1 e 2;*

b) le esenzioni dall'applicazione dell'articolo 97, paragrafi 1, 2 e 3, *sulla base dei criteri stabiliti al paragrafo 3 del presente articolo;*

c) i requisiti che le misure di sicurezza devono soddisfare *conformemente all'articolo 97, paragrafo 3, **per tutelare la riservatezza e l'integrita delle credenziali di sicurezza personalizzate degli utenti di servizi di pagamento**; e*

d) i requisiti per standard aperti di comunicazione comuni e sicure ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni*, nonche dell'attuazione delle misure di sicurezza, tra i prestatori di servizi di pagamento di radicamento del conto, i prestatori di servizi di disposizione di ordine di pagamento, i prestatori di servizi di informazione sui conti, i pagatori, i beneficiari e altri prestatori di servizi di pagamento*

Ruolo cruciale dell'EBA nella definizione dei requisiti di *strong customer authentication* e nella relazione con le Terze Parti

Discussion Paper EBA su Autenticazione e Comunicazione sicura (1/2)

BACKGROUND

✓ Rispetto alle «Norme Tecniche di Regolamentazione (Regulatory Technical Standards – RTS) sull'autenticazione forte del cliente e sulla comunicazione sicura ai sensi della nuova Direttiva sui Servizi di Pagamento (PSD)», data la complessità del tema in oggetto, l'EBA ha posto in consultazione lo scorso 8 dicembre un ***Discussion Paper*** **(DP)** *ad hoc,* con possibilità di inviare le risposte entro l'**8 febbraio**.

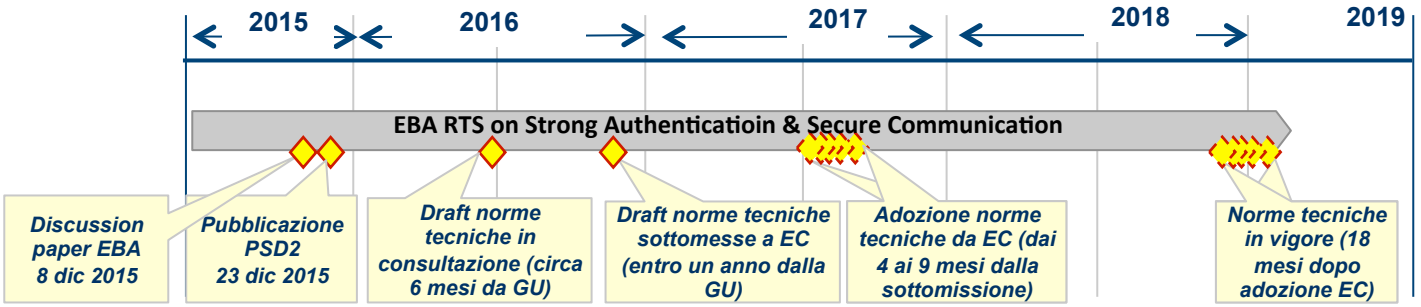
OBIETTIVO DEL DP

✓ Raccogliere **commenti e osservazioni dai principali stakeholder** su alcuni **punti chiave che saranno trattati/chiariti negli RTS**, relativamente all'autenticazione forte del cliente e alla comunicazione sicura.

✓ Nella stesura degli RTS, l'EBA riconosce la complessità della materia e del raggiungimento di un **equo bilanciamento** tra esigenze opposte:

- Elevati requisiti di **sicurezza** vs **semplicità d'utilizzo** dei servizi di pagamento;
- Elevati requisiti di **sicurezza** vs **customer convenience**;
- Elevati livelli di **dettaglio** delle specifiche **tecniche di comunicazione** vs opportunità di lasciare **spazio all'innovazione** non discriminando tra diverse tecnologie.

TEMPISTICHE



La consultazione sugli RTS è attesa per Giugno-Luglio 2016

Discussion Paper EBA su Autenticazione e Comunicazione sicura (2/2)

STRUTTURA DEL DOCUMENTO

✓ Il DP si concentra su **cinque aree specifiche**:

1. **Requisiti di autenticazione forte** del cliente;
2. **Esenzioni dall'applicazione dell'autenticazione forte del cliente** sulla base di criteri prestabiliti;
3. **Requisiti delle misure** di sicurezza per tutelare la **riservatezza e l'integrità delle credenziali personalizzate di sicurezza** degli utenti;
4. **Requisiti** per **standard aperti di comunicazione comuni e sicuri** ai fini dell'identificazione, dell'autenticazione, della notifica e della trasmissione di informazioni, nonché dell'attuazione delle misure di sicurezza, tra i prestatori di servizi di pagamento di radicamento del conto, i nuovi prestatori di servizi dispositivi e informativi, i pagatori, i beneficiari e altri PSP;
5. **Possibili sinergie** con il regolamento sulla identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno (**e-IDAS**).

✓ Per ciascuno dei macro-argomenti, il documento espone:

a) le **norme di riferimento** presenti nella PSD2 (ad esclusione del 5° capitolo);

b) i principali **punti di attenzione** (“Issue”);

c) una serie di **domande aperte** per gli stakeholder, per un totale di 20 quesiti.

RISPOSTA ALLA CONSULTAZIONE

✓ ABI Lab, nell’ambito delle attività predisposte da **ABI**, ha contribuito alla **raccolta** del **punto di vista** delle **banche sui contenuti del DP** e alla **redazione del Position Paper** di risposta inviato all’EBA

Non solo PSD2…

DIRETTIVA NIS

- Direttiva europea sulla **sicurezza di reti e informazioni**, in attesa di approvazione formale dal Parlamento, ha l'obiettivo di:
  - di migliorare le capability in materia di cybersecurity nei diversi Stati Membri, anche attraverso la costituzione di CERT
  - di assicurare la cooperazione e lo scambio di informazioni tra i diversi Paesi
  - di richiedere agli operatori di servizi essenziali e ai provider di servizi digitali "chiave" di introdurre opportune misure di sicurezza e notificare incidenti alle Autorità competenti
- Sulla scia della Direttiva NIS, sono state già definite in diversi Paesi, tra cui l'**Italia**, delle **strategie nazionali di cybersecurity**

GENERAL DATA PROTECTION REGULATION

- Pubblicata il **4 maggio 2016** sulla Gazzetta Ufficiale dell'Unione Europea, da recepirsi in **due anni** dall'adozione **a livello nazionale**
- L'obiettivo è **armonizzare** le **norme sulla privacy a livello europeo** e garantire la **protezione dei dati personali** nell'**era digitale, favorendo** al contempo la **digital economy**
- **Principali elementi di novità:**
  - Diritto all'oblio e alla cancellazione
  - Figura del Data Protection Officer
  - Obbligo di notifica di data breach
  - Diritto di spostare i dati da un prestatore di servizi a un altro
  - Garanzie più rigorose per il trasferimento di dati personali al di fuori dell'UE

La valutazione del rischio informatico

- Sempre maggior attenzione anche sotto il profilo normativo sulle **attività** di **analisi del rischio informatico**, in particolare per gli eventi riconducibili a **FRODE, FURTO e DISCONTINUITÀ DI SERVIZIO** e sui **rischi operativi** correlati
- Al fine di supportare l'attività di gestione del rischio, è opportuno **definire una metodologia di analisi** in grado di **mappare tutte le minacce** che possono impattare sul business e sull'operatività della banca e prevedere le opportune contromisure di contrasto e mitigazione

Eventi di violazione

Rif: COBIT

- Alterazione e manomissione
- Distruzione e danneggiamento
- Divulgazione
- Errori di progettazione e modellizzazione
- Errori operativi
- Interruzione/ indisponibilità
- Sottrazione illecita
- Utilizzo improprio di risorse e facoltà
- Violazione normative e regolamenti

Riconducibili a **FRODE, FURTO e DISCONTINUITÀ DI SERVIZIO**

Minacce di tipo malevolo (generate da attori interni o esterni)

Rif: ISO27005 e CATALOGO BSI

- **Modifica** non autorizzata degli **apparati hardware**
- **Modifica** non autorizzata ai **SO** (inclusi anche attacchi di virus / trojan ai SO)
- **Modifica** non autorizzata al **codice applicativo**, anche in fase di progettazione/ change
- **Modifica** intenzionale dei **dati** non autorizzata
- **Discontinuità** provocate sui **servizi** esterni di connettività fonia e dati
- **Saturazione** della **rete** interna (attacco alla rete interna / flooding / DOS)
- **Cancellazione** intenzionale di **dati** non autorizzata
- **Intercettazione** / **interferenza** delle **comunicazioni**
- **Comunicazione** intenzionale di **dati** non autorizzata
- **Furto** di **apparecchiature** e supporti
- **Furto** di **credenziali** di accesso
- **Furto** o sottrazione di **dati** / data leakage / data loss
- **Abuso** di **privilegi**

Asset impattati

Rif: COBIT

- Applicazioni
- Base dati
- Infrastrutture IT – HW
- Infrastrutture IT – SO
- Infrastrutture IT – Rete
- Risorse Umane/ Organizzazione

Raccordo con Event Type di livello II

Rif: ET Basilea II

- Frode Interna
  - Attività non autorizzata
  - Frode e furto da personale interno
- Frode Esterna
  - Sicurezza dei Sistemi
  - Frodi su carte
- Clienti, prodotti e pratiche di business
  - Relazioni con il cliente
- Danni a beni fisici

Estratto della «Tassonomia minacce ed eventi di rischio informatico», ABI Lab - gennaio 2015

Conclusioni

- L'evoluzione normativa conferma come il legislatore veda **sicurezza cyber** sempre **più strategica**
- L'insieme delle **policy**, delle **misure tecnologiche** adottate e delle **valutazioni del rischio informatico** deve essere ben chiaro e rappresentato ai **vertici aziendali**
- La **gestione del rischio informatico** costituisce sempre di più un'**attività core** della banca che offre servizi digitali

…in prospettiva, è importante che siano seguiti dal legislatore alcuni principi chiave

→ **Avere una prospettiva e un perimetro di applicazione internazionale**, perché la cybersecurity non è un problema «locale»

→ **Assicurare un level playing field tra i diversi competitor**, secondo il principio "same services/ risks, same rules"

→ **Evitare ridondanze e frammentazioni**, creando un framework normativo il più possibile coerente e armonico a livello europeo

→ **Favorire l'information sharing**, per passare dalla logica dell'obbligo di reporting all'opportunità di early warning

→ **Garantire la neutralità tecnologica promuovere l'interoperabilità e gli standard esistenti**, raggiungendo il giusto equilibrio tra innovazione e compliance