SOUTH EASTERN EUROPE

Solutions for Demanding Business

Le minacce informatiche alle transazioni online, come combatterle.
Dall'autenticazione alla prevenzione delle frodi

Asseco Group – Informazioni generali

Ranking dei 100 principali produttori di software in Europa

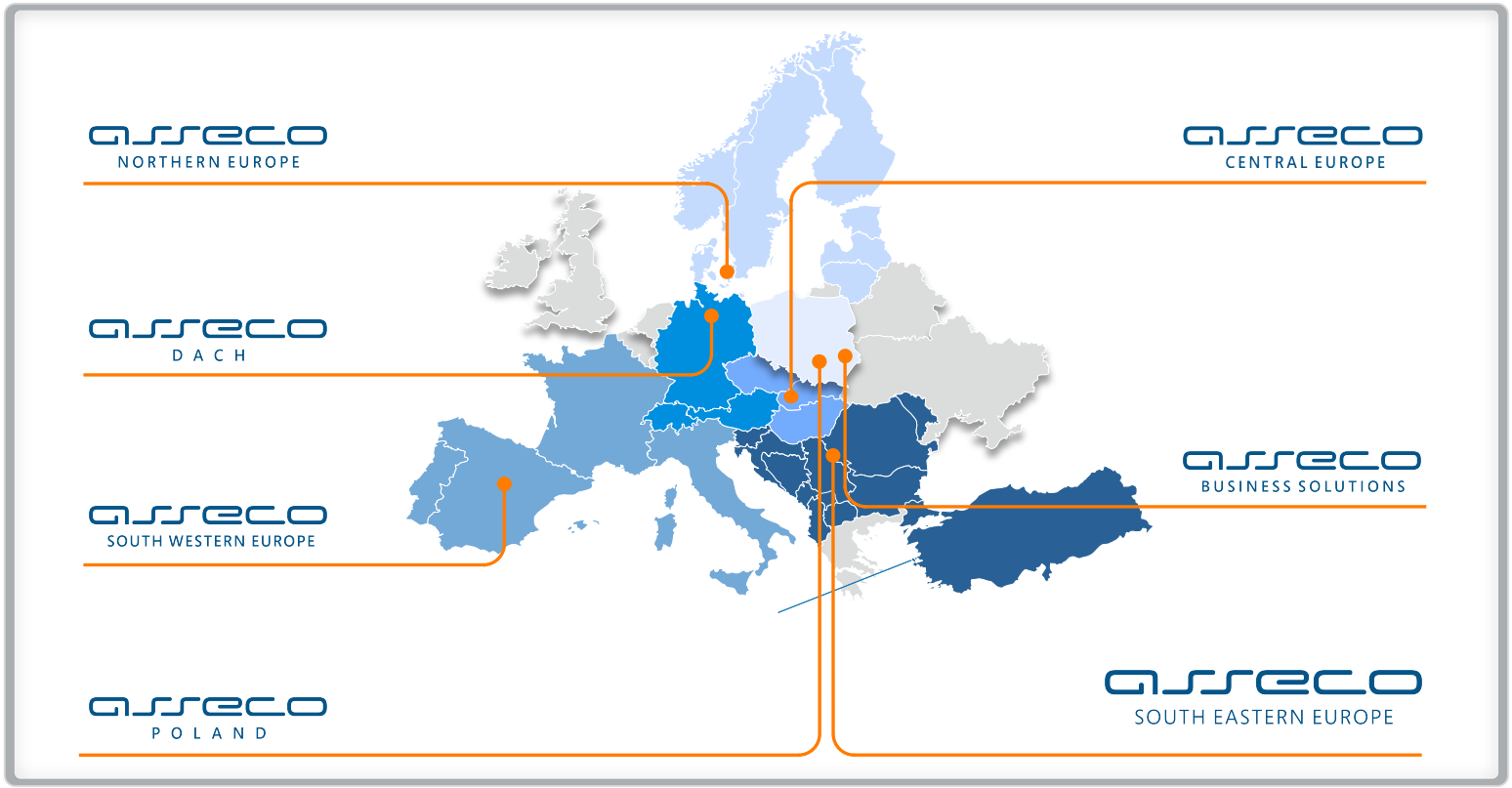
Rank	Company	Country of HQ location	Public	Software +Services 2012 (m€)	Total revenue 2012 (m€)	R&D employees 2012
1	SAP	DE		15 930.0	16 222.0	18 012
2	Dassault Systemes	FR		1 853.4	2 038.5	4 500
3	Sage	UK		1 591.4	1 675.1	1 391
4	Hexagon	SE		1 282.8	2 380.0	3 000
5	Wincor Nixdorf	DE		1 257.3	2 390.3	781
6	Asseco Group	PL		1 002.1	1 320.1	3 180
7	Software AG	DE		922.2	1 047.3	887
8	DATEV	DE		736.7	759.5	1 312
9	Wolters Kluwer	NL		733.4	3 597.0	2 312
10	SWIFT	BE		594.9	597.0	465

Truffle 100

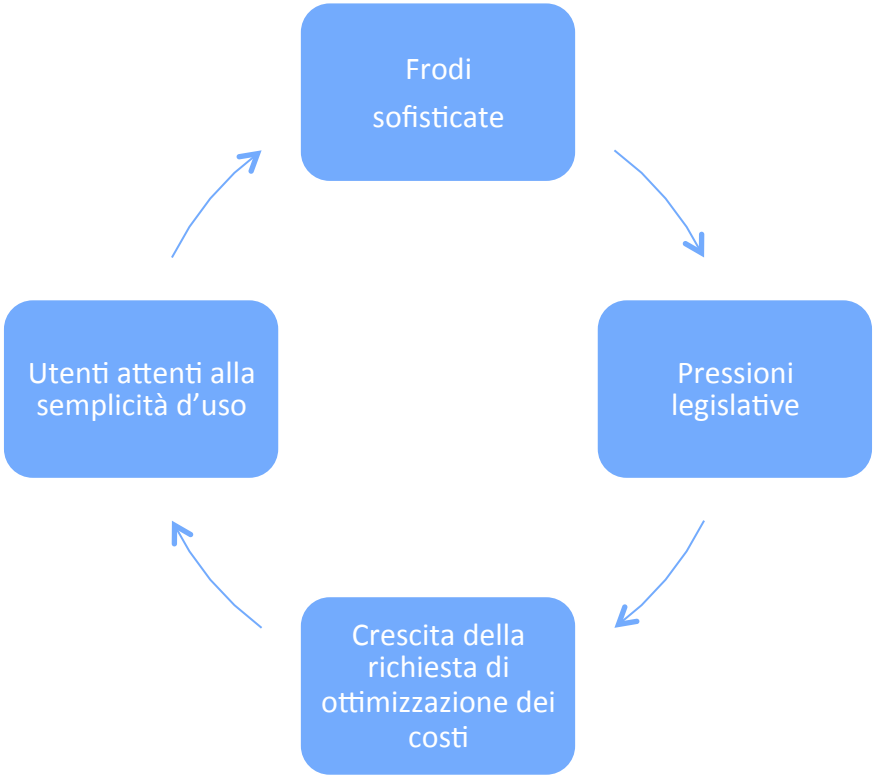
truffle100.com

- 6° produttore di software in Europa
- Azienda in crescita su solide basi
  - Oltre 18.400 dipendenti
  - Profili di business diversificati
  - Concentrata su software e servizi proprietari
- Finanziariamente consistente
  - Ricavi 2014 1,5 MLD EUR
  - CAGR +25.3% (2007-2014)
  - EBIT 2014 153 mil EUR

La nostra presenza in Europa



La sfida della sicurezza nell'e-Banking di oggi



Come affrontiamo questa sfida?

Prevenzione frodi esterne

Autenticazione dell'utente Firma delle transazioni

Prevenzione frodi interne

InAct

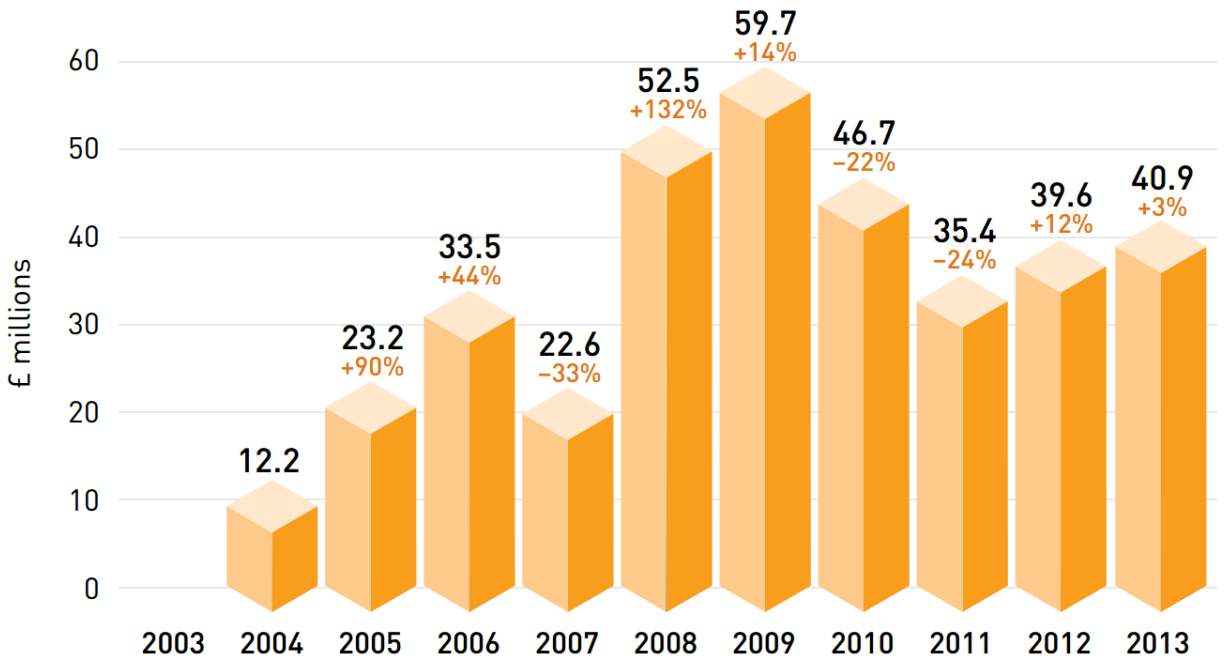
SxS PKI VAS

InAct

Crescita delle perdite da frodi (UK)

Online banking fraud losses 2004-2013

Figures in orange show percentage change on previous year's total



I 3 attacchi informatici più pericolosi contro l'E-Banking

Phishing

Man in the middle (pc, browser, mobile)

Remote Access

Phishing

Phishing - **20 maggio 2015 - Intel Security – il 97% degli utenti non sa riconoscere una e-mail di phishing**

Grande difficoltà da parte degli utenti nel riconoscere le e-mail di phising: è quello che emerge dai dati del Phishing Quiz di Intel, un'indagine volta a testare la conoscenza e l'abilità degli utenti nel riconoscere le e-mail di phishing. Il quiz, formato da 10 email realizzate da Intel Security, ha chiesto agli utenti di identificare quali di esse fossero e-mail legittime e quali, invece, esemplari di phishing progettati per carpire informazioni riservate. Tra i circa 19.000 partecipanti di 144 paesi, solo il 3% è stato in grado di identificare correttamente tutti e 10 gli esempi, mentre l'80% non ha identificato almeno una e-mail di phishing…

- Fonte Intel Security

Man in the middle (browser, pc, mobile)

Subterfuge: attacco man in the middle per tutti in pochi clic

Dimenticatevi Ettercap e procedure “complicate” per effettuare un attacco man-in-the-middle (MITM), con Subterfuge anche un bambino è in grado di rubare le credenziali di autenticazione di un client vittima. Non conoscevo questo tool, ancora giovane, ma è stata una scoperta sorprendente.
Uso da anni Ettercap e lo trovo anche semplice ma Subterfuge lo è ancora di più: ha un’interfaccia Web molto chiara che permette di avviare il MITM e visualizzare in tempo reale username e password intercettate dalle connessioni degli utenti vittime del nostro attacco. Inoltre è dotato di moduli aggiuntivi che ne estendono ulteriormente le funzionalità: fake access point, DNS spoofing, Session Hijacking, HTTP Code Injection, spoofing di un server che invii update.

- Fonte www.bufferoverflow.it

Attacco Remote access

17 dicembre 2014 - Akamai Technologies - Colpiti i sistemi operativi iOS e Android

Gli aggressori colpiscono i dispositivi mobili; durante gli attacchi vengono installati Trojan di accesso remoto per rubare le credenziali di accesso. Akamai Technologies, Inc. (NASDAQ: AKAM), il provider leader di servizi cloud per la distribuzione, l'ottimizzazione e la protezione di contenuto online e applicazioni aziendali, ha pubblicato oggi, tramite il Prolexic Security Engineering & Research Team (PLXsert) dell'azienda, la notifica di una nuova minaccia alla cyber sicurezza. La notifica mette in guardia le aziende, i governi e le singole persone da Xsser mRAT (mobile Remote Access Trojan), un virus che attacca i dispositivi basati su iOS e Android.

- Fonte Akamai Technologies

Come combattere i criminali informatici?

1

Aumentando la sicurezza con sistemi user friendly ma al contempo evoluti di autenticazione e tool di analisi delle transazioni "cross-channel".

2

Formando adeguatamente il proprio personale e, soprattutto, sensibilizzando la clientela, affinchè percepiscano il valore della sicurezza.

Cosa dovrebbero fare le Banche in futuro?

1. Dotarsi di strumenti di autenticazione con funzioni di host verification e firma delle transazioni;

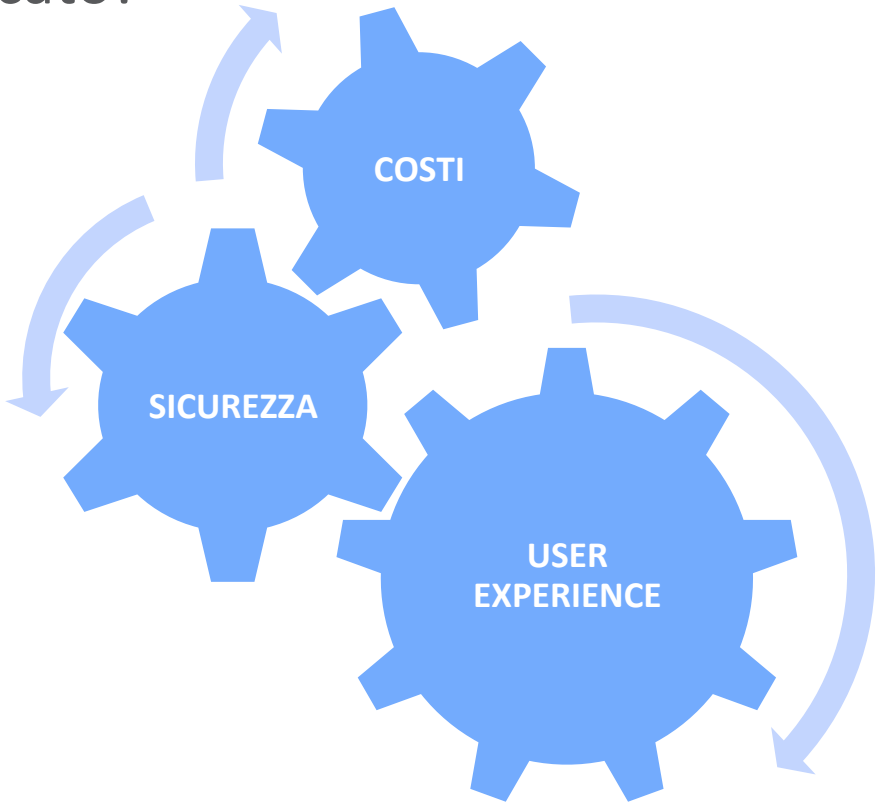
2. Utilizzare metodi di autenticazione adattativi;

3. Implementare sistemi Anti-frode basati sull'analisi del comportamento e dei rischi;

4. Adottare soluzioni economicamente efficienti per proteggere il loro business;

5. Adeguarsi alle linee guida normative, presenti e future, della BCE e di Banca d'Italia.

L’equilibrio è delicato!



Cosa abbiamo fatto per aiutare le Banche? ASEBA SxS

- Soluzione di autenticazione con funzioni di host verification e firma delle transazioni
- Metodi e strumenti di autenticazione diversificati e adeguabili alle necessità di business

Cosa abbiamo fatto per aiutare le Banche? ASEBA Mobile Token

- Strumenti di autenticazione con funzioni di host verification e firma delle transazioni

QR Code Dig Sig & Host Verification

Firma della transazione (MAC/MDS):

Nome – IBAN - Importo – Valuta - Data

QR code firmato

Input sempice nel mobile token

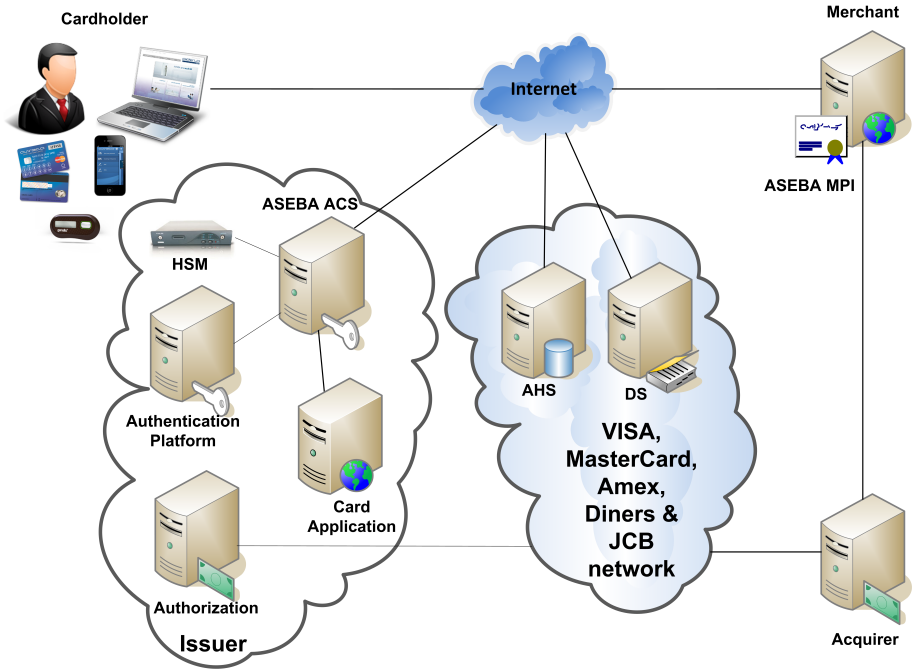
Localizzazione dell'utente on-line in tempo reale SIM-based

Distribuzione delle Mobile Apps con meccanismi anti malware

Utilizzo della biometria (impronta digitale) per lo sblocco delle Apps

Cosa abbiamo fatto per aiutare le Banche? ASEBA TriDes

- Soluzione di autenticazione 3Dsecure per le transazioni di E-Commerce
- Consente l'impiego di dispositivi di autenticazione coerenti con quelli in uso per l'E-Banking



Cosa abbiamo fatto per aiutare le Banche? ASEBA InAct

- Soluzione Anti-frode centralizzata basata sull'analisi del comportamento dell'utente;
- Solo controllo? NO! Reazione in tempo reale: Autenticazione adattativa!

InACT®

Data Management

- Risposte in Real Time
- Trasferimento dati on-line in Near Real Time
- Trasferimento dati in Batch
- Caricamento file Esterni

InACT®

Scoring

- Risultati degli Scenari results (allarmi)
- Calcolo degli Score

InACT®

Management

- Tabelle e colonne
- Gestione utenti
- Assegnazione dinamica
- Template testi
- WFL

InACT®

Scenari

- SQL Wizard
- Definizione Scenari
- Definizione Statistiche (RT e batch)

InACT®

Analisi

- Analisi Allarmi (frodi utenti e commercianti)
- Azioni
- Analisi POC
- Dashboard

InACT®

Case Management

- Gestione casi
- Assegnazione casi
- Chiusura casi

InACT®

Reports

- Reports personalizzati
- Reports preconfigurati

InACT®

Chiusure

- Pulizia quotidiana degli scripts

Cosa abbiamo fatto per aiutare le Banche?

- User Case, sfide del business:
  - CIB – (Gruppo Intesa San Paolo)
  - Riduzione delle frodi legate a OTP via SMS
  - Riduzione dei costi
  - Svincolo dal singolo vendor di dispositivi
- In produzione da Agosto 2013
- Installato:
  - SxS authentication Server
  - Mobile token
  - VASCO Migration program

- 100.000 nuovi OTP tokens Gemalto OATH, 100.000 Mobile tokens, supporto ai tokens VASCO DP 260 esistenti

Cosa abbiamo fatto per aiutare le Banche?

- User Case, sfide del business:
  - PBZ Croazia (Gruppo Intesa San Paolo)
  - Gestione omogenea di dispositivi diversificati
  - Riduzione dei costi
  - Svincolo dal singolo vendor di dispositivi

- In produzione da: Fase 1 – 2001 / Fase 2 – 2005 / Fase 3 - 2007

- Installato:
  - SxS authentication Server con HSM Thales
  - Mobile token

- 400.000 utenti: HW tokens ActivIdentity, Mobile token Asseco, Cap Reader Xiring/Gemalto, PKI con certificati governativi

Cosa abbiamo fatto per aiutare le Banche?

- User Case, sfide del business:
  - RBA Croazia
  - Autenticazione centralizzata per linee di business diverse:
    - Internet Banking – E-commerce – Phone banking
  - User experience unica sui diversi canali

- Prima implementazione 1997 (in costante evoluzione)

- Installato:
  - SxS authentication Server con HSM Thales
  - Mobile token

- Circa 200.000 utenti: HW tokens ActivIdentity, MToken Asseco, Cap Reader Xiring.

Perché Credem ha scelto Asseco-SEE?

1. Per la flessibilità dimostrata dalle soluzioni di autenticazione e anti-frode che le permettono di affrontare le nuove sfide del mercato;
2. Per la volontà dimostrata dalla nostra azienda nel soddisfare le esigenze della banca;
3. Per gli eccellenti risultati ottenuti nella frase preventiva di test (PoC).

CREDEM

Perché le banche italiane dovrebbero scegliere Asseco-SEE?

- Asseco SEE ha molti anni di esperienza nel campo della sicurezza delle transazioni on-line, maturata dalla relazione con le oltre 70 banche nel mondo, clienti in questo settore;

- Asseco SEE è in grado di preservare gli investimenti, fatti dai propri clienti negli anni, sia sui dispositivi di autenticazione, sia nelle applicazioni di Mobile Banking;

- Asseco SEE è alla costante ricerca dell'innovazione nel campo del contrasto alle frodi, e i suoi prodotti anticipano spesso le esigenze dei suoi clienti.

Key References - Banking & Financial

Key References – Banking, Financial, Payments

Grazie