Conferenza ABI "Banche & Sicurezza 2015"

Roma, 05 Giugno 2015

MARKETING & CYBER INTELLIGENCE NEL SETTORE BANCARIO FRANCESE: ESPERIENZE SUL CAMPO

Jamil Ouazzani

Partner Easy Business in Milan

Tutte le organizzazioni, anche quelle dotate dei più importanti sistemi di sicurezza, possono subire attacchi informatici.
Ma alla fine è sempre l'azienda la responsabile dei problemi di sicurezza.

Gli argomenti di oggi…

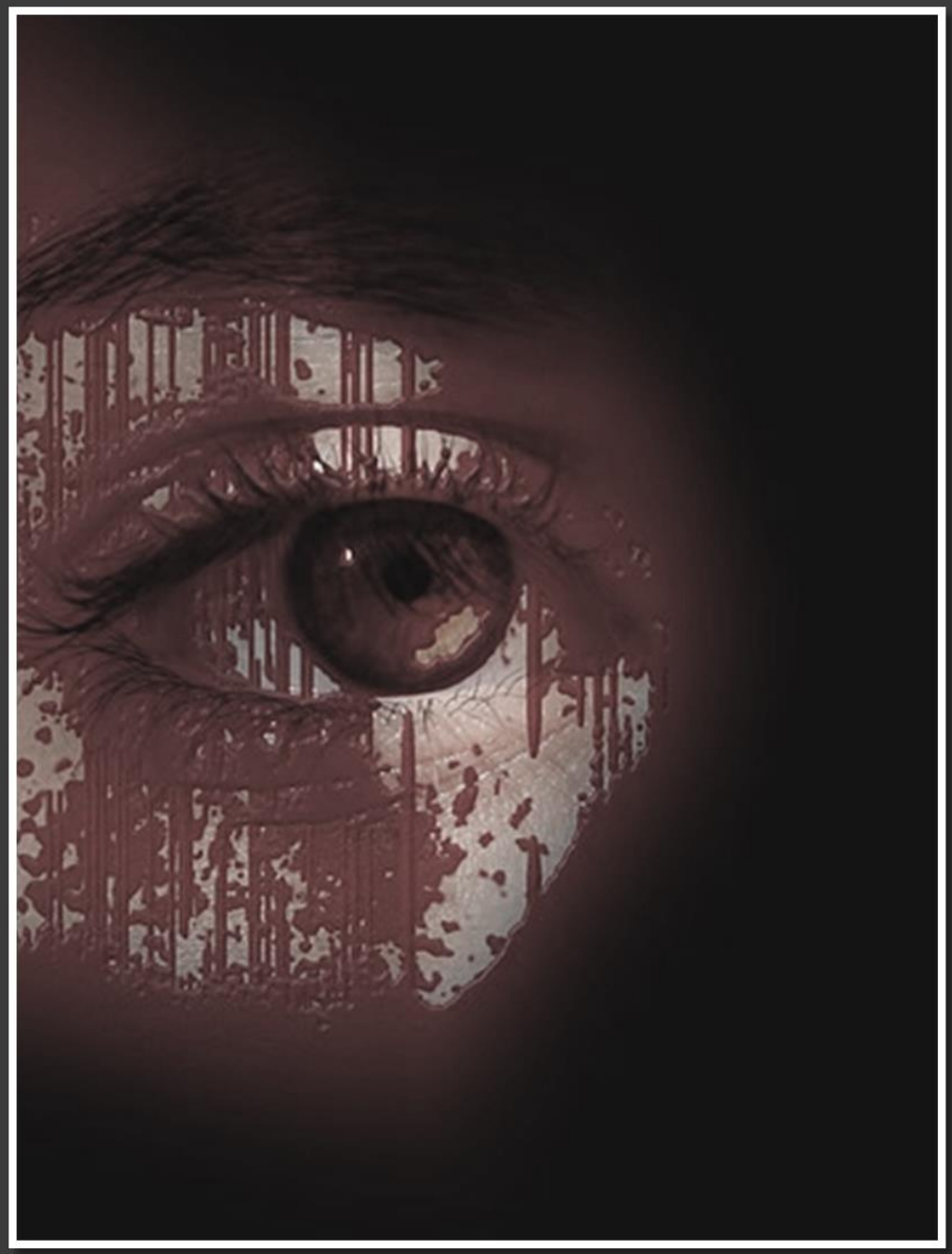
- Il mondo bancario francese
- La cyber criminalità in Francia
- La cultura oltralpe dell'intelligence e il ruolo del Marketing & Competitive Intelligence
- Il dilemma delle banche
- L'approccio del Gruppo Bancario "X" per la gestione della cyber security

Il mondo bancario francese

Il mondo bancario francese

- **390** banche
- **37.862** filiali
- **371.000 dipendenti** che lavorano per un **70% nelle filiali** (Agenzia)
- **99% dei francesi** hanno un conto bancario
- **71 milioni** di conti correnti
- **58.641** sportelli ATM
- **87% dei francesi** si recano almeno una volta in banca durante l'anno
- **7 internauti su 10** si connettono online con la loro banca (home banking)
- **18 miliardi** di operazioni relative a pagamenti
- **49,5%** dei pagamenti sono effettuati con una carta di pagamento
- **82,2 milioni** di carte di pagamento in Francia (759,6 milioni in Europa)
- **56% degli internauti** utilizzano la loro carta bancaria per i pagamenti online

Fonte: Fédération Bancaire Française (2015)



La cyber criminalità in Francia

La cyber criminalità in Francia

- Non abbiamo trovato, nei vari paesi del mondo, una definizione ufficiale della cyber criminalità. Questo termine è presente in più punti nel Codice Penale francese senza offrirne una definizione precisa ed include* tutte le infrazioni informatiche e così dette di contenuto come la pedopornografia In ogni caso, parliamo di "*infrazioni penali tentate o commesse ai sistemi informatici e di comunicazione, principalmente attraverso la rete internet*".
- Queste infrazioni sono sanzionate dal Codice Penale come ad esempio
  - Gli attacchi ai Sistemi di Trattamento Automatizzato dei Dati (S.T.A.D) ➔ sanzionati con gli art. L.323-1 e succ. del Codice Penale
  - Le violazioni relative al diritto delle persone effettuate attraverso la rete ➔ art. 226-16 a 226-24 del Codice Penale / Legge 78-17 del 06 Gennaio 1978 modificata con la legge 2004-801 del 06 Agosto 2004 (informatica e libertà)
  - Le violazioni sui minori (art.227-23 del Codice Penale), sulle persone (minacce, usurpazione di identità, …), le truffe (phishing, pagamenti, …)

* anche se la cybercriminalità non si limita solo ad Internet che appare oggi come il suo principale vettore.

Fonti: ANSSI e Ministère de la Justice Française (2015)

La cyber criminalità in Francia

- L'evoluzione della tecnologia e l'utilizzo crescente della rete e dei social network ha portato a forme diverse di cyber attacchi con attività di:
  - Spamming,
  - Phishing (pesca dei dati sensibili),
  - Pharming,
  - Hacking (verso infrastrutture e-commerce, e-banking, …)
  - Malware (trojan, password stealer, …)
  - Skimming
  - Spionaggio industriale,
  - "Man in the middle" (intromissione nelle comunicazioni tra 2 parti per trarne vantaggio: false richieste, …)
  - Molestie, Riscatti e diffamazioni online, …

- Lo Stato francese è sensibile in tutte le tematiche legate alla protezione dei dati personali e finanziari presenti in rete (usurpazione) e all'assicurazione della tracciabilità dei beni (e-commerce).

* Nome e cognome, fotografie, indirizzi mail, indirizzi IP, username e password, CVS

Fonte: Ministère de la Justice Française (2015)

La cyber criminalità in Francia

Alcuni player

- **L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication** (OCLCTIC) è l'organismo della Direzione Centrale della Polizia Giudiziaria francese che si occupa della lotta alla cyber criminalità. È una divisione preposta che fa parte della Direzione della Lotta contro la Criminalità Organizzata e del Crimine Finanziario (SDLCODF).
- L'**OCLCTIC** è stato creato il 15 Maggio 2000; la sua area di interesse è sia nazionale che internazionale. Il personale proviene esclusivamente dalla Scuola di Polizia o dalla Scuola di Gendarmeria con delle competenze, per i funzionari provenienti dalla
  - Polizia, del brevetto ICC (Investigatore in Cyber Criminalità)
  - Gendarmeria, la formazione N-tech (formazione nelle nuove tecnologie)

Fonte: Ministère de l'Intérieur (2015)

La cyber criminalità in Francia

Alcuni player

- Tra le principali attività dell'**OCLCTIC**, troviamo
  - ✓ le indagine giudiziarie per le infrazioni tecnologiche
  - ✓ la formazione e la sensibilizzazione alla tematica della Cyber Criminalità
  - ✓ La cooperazione internazionale con altri organismi
  - ✓ Le attività di Competitive Intelligence
  - ✓ Le altre attività strategiche relative alla tematica
- Questo ufficio collabora con la **B.E.F.T.I** (*Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information*), la **D.C.R.I** (*Direction Centrale du Renseignement Intérieur*), la Gendarmeria Nazionale e la Dogana.

Fonte: Ministère de l'Intérieur (2015)

La cyber criminalità in Francia

Dal 2009 è disponibile

- Un numero di telefono per dare ai cittadini vittime delle frode i primi consigli
- La piattaforma **PHAROS** (**P**lateforme d'**h**armonisation d'**a**nalyse, de **r**ecoupement et d'**o**rientation des **r**enseignements) per denunciare comportamenti o illeciti in rete.

Tutte le richieste sono prese in esame e successivamente inviate ai servizi di competenza: Polizia; Gendarmeria; Direzione Generale della Concorrenza, del Consumo, della Repressione delle frode.

Interpol viene interpellato nel caso di siti ospitati su server esteri.

Fonte: Ministère de l'Intérieur (2015)

La cyber criminalità in Francia

Alcuni player

- L'**A.N.S.S.I** (*Association Nationale de Sécurité des Systèmes d'Information*) è un'entità collegata al Segretario Generale della Difesa e della Sicurezza Nazionale (S.G.D.S.N) a sua volta incaricata ad assistere il Primo Ministro nell'esercizio delle sue funzioni in materia di Difesa e di Sicurezza Nazionale.
- Davanti alle nuove sfide economiche e all'evoluzione continua degli attacchi informatici, l'Associazione si dedica ad accompagnare
  - i privati con delle attività di sensibilizzazione per la protezione dei dati personali
  - le aziende con delle attività di consulenza personalizzate in cyber security

  e, allo stesso momento, promuove con delle politiche industriali e di regolamentazione la conoscenza dei prodotti e servizi di cyber sicurezza affidabili.

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- L'**A.N.S.S.I** ha pubblicato nel 2011 la *Strategia della Francia in materia di Difesa e di Sicurezza dei Sistemi Informatici:*
  - *http://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/*
- La strategia di intervento della Francia per prevenire e garantire la sicurezza delle aziende pubbliche o private e dei cittadini in caso di cyber criminalità si focalizza su 4 obiettivi precisi
  1. Diventare una potenza mondiale di cyber difesa e appartenere al circolo delle nazioni più importanti conservando tuttavia la propria autonomia
  2. Garantire la libertà di decisione della Francia per la protezione della dell'informazione
  3. Rinforzare la cyber security delle infrastrutture vitali nazionali
  4. Assicurare la sicurezza nello cyber spazio

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- L'ANSSI è divisa in 2 direzioni:
  - La Direzione *Affari generali* e la Direzione *Strategia*
- La Direzione *Affari Generali* è a sua volta suddivisa in 4 sotto direzioni:
  - Il Centro Operativo della Sicurezza dei Sistemi di Informazioni (**COSSI**)
  - La sotto-direzione *Expertise* (**SDE**) che lavora anche con gli altri Ministeri, le industrie, le società specializzate in sicurezza e gli operatori strategici
  - La sotto-direzione *Systèmes Informations Sécurisés* (**SIS**) che ha come missione di proporre e offrire dei prodotti e sistemi di informazioni "sicuri" non solo per l'ANSSI ma anche per i Ministeri e per gli operatori strategici
  - La sotto-direzione *RELations Extérieures et Coordination* (**RELEC**)

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- Il Centro operativo della Sicurezza dei Sistemi Informazioni (**COSSI**) si dedica particolarmente a tutte le Amministrazioni Pubbliche e a tutti gli operatori strategici del paese (classificati come "operatori di importanza vitale" per la Nazione)
- È allo stesso momento responsabile
  - dell'analisi delle minacce
  - dell'identificazione delle vulnerabilità dei sistemi o dei prodotti in uso
  - della ricerca, qualificazione e modalità di risposta degli attacchi in corso
  - dell'accompagnamento per l'applicazione delle misure di correzione urgenti.

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- Il Piano **Vigipirate** è sotto la tutela del Primo Ministro e coinvolge tutti i Ministeri. È uno strumento centrale del dispositivo di difesa francese creato per contrastare le azioni terroristiche e per mantenere alto il livello di guardia davanti a queste minacce.
  - È un dispositivo costantemente attivo di vigilanza, prevenzione e protezione che viene programmato nel paese ma anche all'estero a diversi soggetti: Lo Stato, le collettività territoriali, gli operatori dedicati alla sorveglianza e alla protezione, ed infine ai cittadini.
  - Il Piano si applica a molti settori di attività: trasporti, sanità, alimentazione, energia,… cercando di non influire sulla vita economica e sociale del paese.
- Il Piano **Piranet** è complementare al Piano Vigipirate e serve alle famiglie in caso di attacchi informatici rilevanti.

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- Gli **O**sservatori di **z**ona per la **S**icurezza dei **S**istemi di **I**nformazioni (**OzSSI**) sono stati creati dal Ministero dell'Interno e servono a rinforzare a livello locale le azioni prese per la difesa dei sistemi informatici.
- Il territorio francese è stato suddiviso in aree di difesa: **Iles de France**, **Zona Est** della Francia (Alsazia, Borgogna, Champagne-Ardennes, France Comté e Lorraine), **zona Nord** (Nord Pas de Calis e Picardie), **zona Ovest** (Bassa Normandia, Bretagna, Centro –Alta Normandia e Paesi della Loira), **zona Sud** (Corsica, Languedoc, Provence Alpes Cote d'Azur), **zona Sud Est** (Auvergne, Rhone Alpes) e **zona Sud Ovest** (Acquitaine, Limousin, Midi Pyrénées e Poitou Charrentes).

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

Alcuni player

- I **CERT (*Computer Emergency Response Team*)** sono degli organismi ufficiali accreditati che svolgono un ruolo di assistenza ma allo stesso momento allertano e presentano alle aziende pubbliche e private delle contromisure agli attacchi informatici.
- Esistono diversi CERT in Francia come ad esempio
  - Il CERT-FR dell'ANSSI
  - CERT-Société Générale
  - CERT Crédit Agricole
  - CERT BNP Paribas
  - CERT BDF (Banque de France)

La cyber criminalità in Francia

Premier ministre

Agence Nationale de la Sécurité des Systèmes d'Information

CERT-FR

Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques

Informations utiles
Que faire en cas d'intrusion ?
Les systèmes obsolètes
Liens utiles

L'ANSSI recrute

Les documents du CERT-FR
Publications récentes
Les alertes en cours
Les bulletins d'actualité
Les notes d'information
Année en cours

Les Flux RSS du CERT-FR
Flux RSS complet
Flux RSS des alertes
Flux RSS SCADA

ACTUALITÉS

Protéger son site Internet des cyberattaques

ALERTES (LES 5 PLUS RÉCENTES)

Les alertes sont des documents destinés à prévenir d'un danger immédiat.

CERTFR-2015-ALE-004	Vulnérabilité dans Microsoft Internet Explorer (**Corrigée le 31 mars 2015**)
CERTFR-2015-ALE-003	**Nouvelle campagne d'hameçonnage de type rançongiciel (06 février 2015)**
CERTFR-2015-ALE-002	Vulnérabilité dans Adobe Flash Player (**Corrigée le 05 février 2015**)
CERTFR-2015-ALE-001	Vulnérabilité dans Adobe Flash Player (**Corrigée le 30 janvier 2015**)
CERTFR-2014-ALE-011	Vulnérabilité de l'implémentation Kerberos dans Microsoft Windows (**Corrigée le 30 janvier 2015**)

AVIS (LES 20 PLUS RÉCENTS)

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

CERTFR-2015-AVI-224	Vulnérabilité dans Xen (13 mai 2015)
CERTFR-2015-AVI-223	Multiples vulnérabilités dans Wireshark (13 mai 2015)
CERTFR-2015-AVI-222	Multiples vulnérabilités dans Adobe Flash Player (13 mai 2015)
CERTFR-2015-AVI-221	Multiples vulnérabilités dans les produits Mozilla (13 mai 2015)
CERTFR-2015-AVI-220	Vulnérabilité dans la bibliothèque Schannel de Microsoft Windows (13 mai 2015)

Fonte: CERT-FR (2015)

La cyber criminalità in Francia

Raccomandazioni in caso di sospetti o di incidenti

- Sospetto per un eventuale attacco informatico:
  - ➔ www.cert.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html
- Ricezione di mail non sollecitate:
  - ➔ Utilizzare Signal-Spam: www.signal-spam.fr/
- Ricezione di messaggi con contenuti inappropriati:
  - ➔ Utilizzare il sito Internet-signalement-gouv.fr: www.internet-signalement.gouv.fr

Per denunciare un caso di cyber criminalità nel caso di

- Infrazioni alle tecnologie informatiche e di Comunicazioni (STAD, File informatici, …)
- Infrazioni legate/facilitate grazie all'utilizzo di tecnologie informatiche e di Comunicazioni
  - ➔ Rivolgersi alla Polizia o alla Gendarmeria* o inviare una lettera al Procuratore della Repubblica Francese presso il TGI (Tribunal de Grande Instance)
  - ➔ È possibile rivolgersi a dei servizi specializzati per la gestione giudiziaria della cyber criminalità

* La Polizia e la Gendarmeria hanno messo a disposizione una rete di investigatori in Cyber criminalità (ICC/Police e N-Tech/Gendarmeria)

Fonte: A.N.S.S.I (2015)

La cyber criminalità in Francia

La situazione nel mondo

- Troels Oerting, ex Direttore dell'EC3 (Europol's European Cyber Crime Unit) parlava durante una sua intervista alla BBC nel 2014 dell'esistenza di circa un centinaio di individui "*responsabili della cybercriminalità nel mondo*".

  ➔ Questo numero ristretto, ben conosciuto dai suoi servizi era secondo il suo punto di vista destinato ad aumentare molto rapidamente a causa delle loro risorse a disposizione e della mancanza di ostacoli per contrastarle.

- La rete è diventata oggi il principale veicolo per la vendita di programmi malvagi di tutti i tipi a criminali presenti in tutto il mondo e in questo caso, diventa facile, grazie ad un download, diventare un cybercriminale senza nessuna competenza tecnica.

La cyber criminalità in Francia

La situazione nel mondo

- Quantificare il fenomeno della cybercriminalità è molto difficile perché bisognerebbe dare prima, a livello internazionale, la stessa definizione "legale" delle infrazioni (Diritto internazionale). In Francia, la rilevazione statistica del Ministero della Giustizia è diversa da quella del Ministero dell'Interno che opera in maniera più globale.
- Rob Wainwright, Direttore di Europol dichiarava pochi giorni fa all'AFP: "*La minaccia online è enorme, ed è attualmente la più grande preoccupazione per la Sicurezza insieme al Terrorismo*".
- Occorre non dimenticare tutte le attività di spionaggio industriale dove, secondo la Comunità Europea, più del 25% delle aziende europee sono state colpite (furto di informazioni strategiche e confidenziali // intelligenze economica).

La cyber criminalità in Francia

Alcuni numeri sulla cybercriminalità in Francia

- Il sito Signal Spam ha ricevuto 2.454.369 segnalazioni nel 2012
- L'AFMM (*Associazione Francese Multimedia Mobile*), più di 5 milioni di segnalazioni (attacchi verso i mobile pervenuti in data 01.09.2012)
- L'Associazione *Phishing Initiative* ha ricevuto circa 50.000 segnalazioni nel 2012 (2/3 delle URL ospitavano contenuti fraudolenti classificati come Phishing).
- La Piattaforma PHAROS ha per conto suo ricevuto nel 2013 22.000 segnalazioni (Phishing).
- Secondo il CREDOC (*Centre de Recherche pour l'étude et l'Observation des Conditions de vie*), assistiamo in Francia a più di 300.000 di furti d'identità online

La cyber criminalità in Francia

Alcuni numeri sulle frode bancarie in Francia

- Le frode bancarie (dati 2012 del Rapporto sulla Cybercriminalità):
  - 125€ = l'ammontare medio di una transazione fraudolente
  - Il danno subito è nel
    - 27% dei casi uguale o inferiore a 100€, nel
    - 25% dei casi, compreso tra 100€ e 300€
    - 29% dei casi, tra 300€ e 1000€
    - 19% superiore a questi importi
  - 767.000 carte di credito sono state bloccate a seguito di transazioni fraudolente
  - Sondaggio INSEE/ONDRP effettuato nel 2013 in Francia:
    - 70% delle famiglie si sono rese conto della frode consultando il loro estratto conto e 22% i loro sono stati avvertiti dalla loro banca.
    - 56% ignorano in che modo i cyber criminali hanno sottratto le loro credenziali bancarie.
    - Nel 2011, 42% delle famiglie hanno denunciato una frode e 77% sono stati rimborsati dalla banca (7% si sono visti rifiutare il rimborso).

La cyber criminalità in Francia

La sicurezza delle carte di pagamento

L'Osservatorio della sicurezza delle carte di pagamento (*Observatoire de la sécurité des cartes de paiements*), presidiato da Christian Noyer, Governatore della *Banque de France* ha pubblicato nel 2014 il suo report annuale sullo stato dell'arte del settore (anno di riferimento 2013).

La cyber criminalità in Francia

La sicurezza delle carte di pagamento

- In sintesi, il tasso di frode per i pagamenti e i prelievi tramite carte di pagamento rimane stabile al 0,080% (anno 2013)
- Per le transazioni nazionali:
  - Il tasso di frode per i pagamenti nazionali attraverso il canale Internet è del 0,229%, in leggera diminuzione rispetto al 0,290% del 2012 (anche se 1/3 di questa diminuzione è da attribuire ad una nuova modalità di rilevazione dei dati → pagamento a distanza via internet o tramite posta / telefono)
  - L'ammontare delle frode sui pagamenti a distanza continua ad aumentare, soprattutto per quelli effettuati via web (→ I pagamenti a distanza corrispondono alla maggior parte delle frode (64,6%) e rappresentano l'11% dell'ammontare del totale delle transazioni).

Fonte: Observatoire sur la sécurité des cartes de paiements (2014)

La cyber criminalità in Francia

La sicurezza delle carte di pagamento

- Per le transazioni internazionali, il tasso di frode si è abbassato anche se questo risultato è da valutare con altre tendenze:
  - Il tasso di frode per i pagamenti effettuati in Francia con carte di credito emesse fuori dalla SEPA (*Single Euro Payments Area*) si è abbassato notevolmente grazie anche alla divulgazione dello standard EMV (Europay Mastercard Visa)

mentre

  - Il tasso delle frode sui pagamenti a distanza effettuati nella zona SEPA con carte di pagamento francesi è aumentato notevolmente. Le raccomandazioni sulla Sicurezza dei pagamenti via web presentate al Forum Europeo sulla Sicurezza dei Pagamenti "SecuRe Pay", dovrebbero migliorare questa situazione negativa.

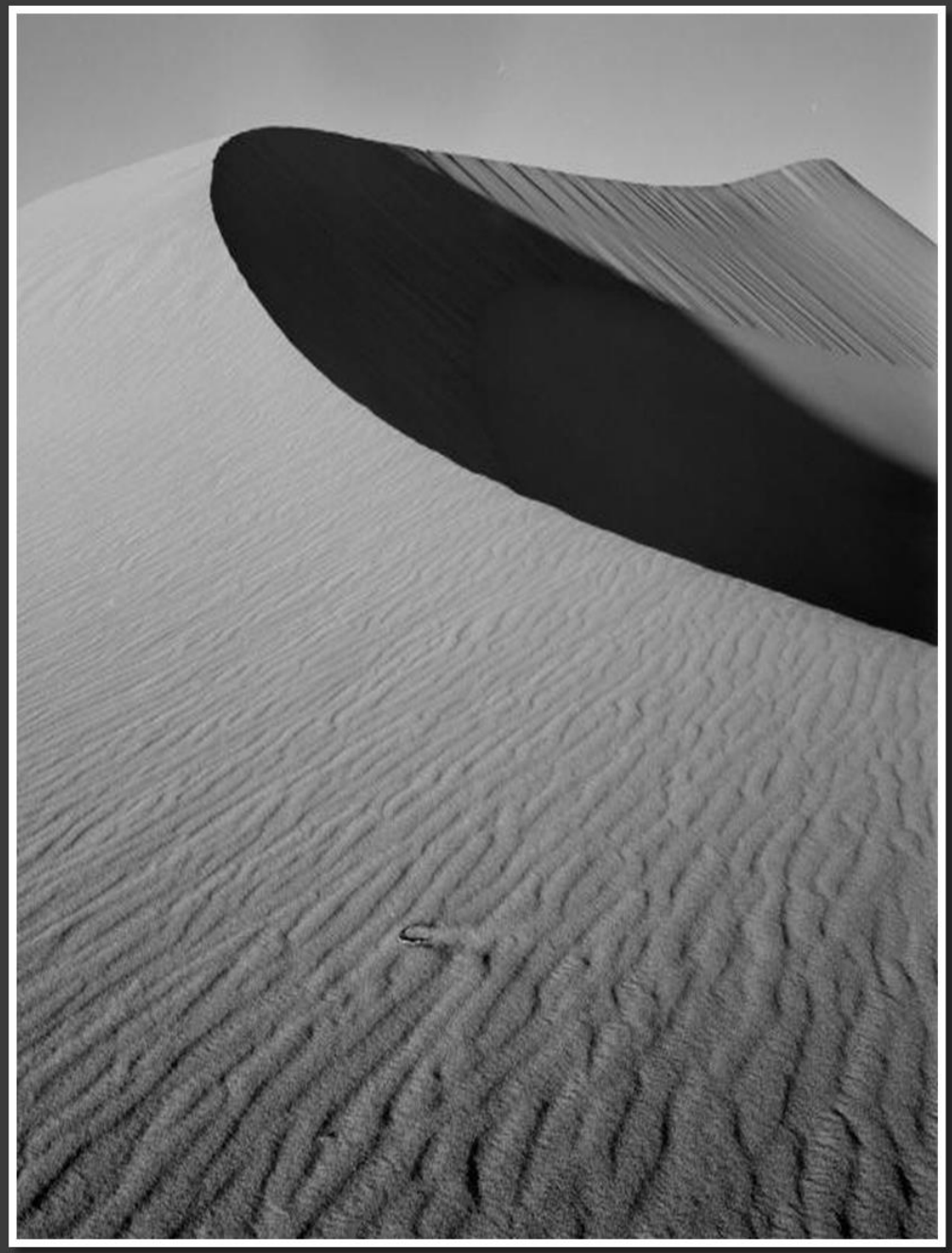
Fonte: Observatoire sur la sécurité des cartes de paiements (2014)

La cyber criminalità in Francia

La sicurezza delle carte di pagamento

- Il numero di manomissioni dei terminali di pagamento è aumentato negli ultimi anni. Per questo motivo, l'Osservatorio sta riesaminando le raccomandazioni presentate nel suo penultimo report chiedendo a tutti i protagonisti coinvolti di stare molto attenti alle eventuali frode. Allo stesso momento auspica un maggior rinforzamento dei sistemi di sicurezza delle transazioni (tecniche di autentificazione e di sicurezza)
- La non esistenza di uno standard EMV per i pagamenti a distanza pone il problema sulla sicurezza dei dati personali (richiesta di inserimento dei dati personali per accertare la propria identità). La **CNIL** (*Commission Nationale de l'Informatique et des Libertés*) sta lavorando su questa tematica puntando su un sistema di autorizzazione unico per migliorare la sua efficacia.
- L'Osservatorio raccomanda ai commercianti di utilizzare dei sistemi di protezione come il servizio 3D Secure

Fonte: Observatoire sur la sécurité des cartes de paiements (2014)

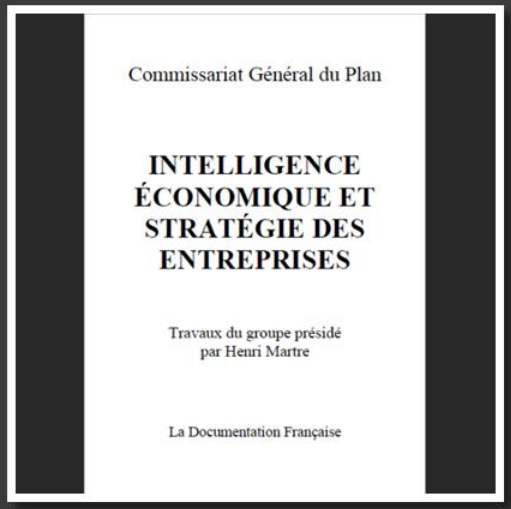


La cultura dell’intelligence e il ruolo del M.C.I

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DÉLÉGATION INTERMINISTÉRIELLE À L'INTELLIGENCE ÉCONOMIQUE

09 Novembre 1989



1994

Giugno 2013

- "La Délégation interministérielle à l'intelligence économique (D2IE) esercita una missione generale di animazione e coordinamento delle azioni dello Stato Francese in ambito di Intelligenza Economica... "
- "L'Intelligenza economica (IE) consiste a raccogliere, analizzare, valorizzare, difondere e proteggere l'informazione economica strategica, con l'obiettivo di rinforzare la compétitività dello Stato Francese, di un'azienda o di un Istituto di ricerca."

Fonte: Délégation Interministérielle à l'Intelligence Economique 2015

La cultura dell'intelligence e il ruolo del Marketing & Competitive Intelligence

Nel mondo della globalizzazione, la gestione "pro-attiva" delle informazioni strategiche è diventata per tutte le Nazioni che l'hanno programmata negli ultimi decenni, uno strumento efficace per competere sui mercati nazionali ed internazionali: Giappone, Stati Uniti, Germania, Francia, Regno Unito, Svezia, Israele, Turchia, Cina, Korea,…

Il **Marketing intelligence** ha come obiettivo il miglioramento della Performance marketing delle aziende (pubbliche o private) mentre la **Competitive intelligence** si focalizza soprattutto sull'analisi dell'ambiente esterno: Mercato, clienti, concorrenti, aspetti normativi, novità tecnologiche, …

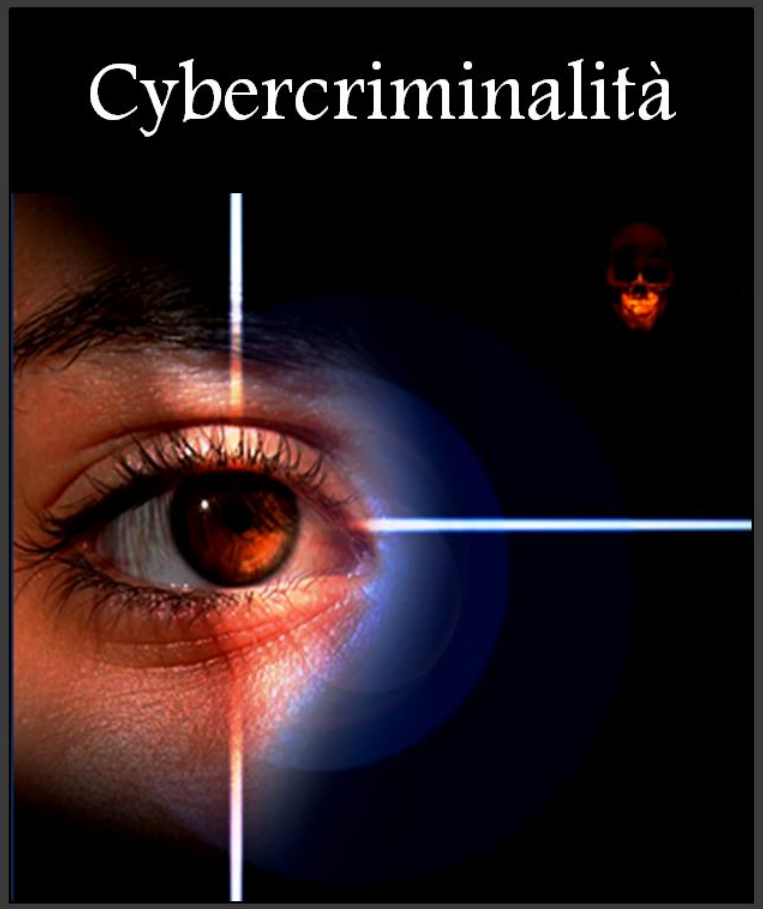
La gestione strategica delle informazioni pertinenti crea inizialmente **Valore** e successivamente diventa fonte di **vantaggio competitivo** e di **Potere**.

La cultura dell'intelligence e il ruolo del Marketing & Competitive Intelligence

Lo sviluppo della tecnologia e dei mezzi di comunicazione hanno cambiato le dinamiche di *Governance* e di *Leadership* nel mondo globale. Oggi, tutte le attività di Risk Management e di Cyber Security dovrebbero rientrare nei budget annuali di sviluppo di tutte le tipologie di Organizzazioni (banche comprese).

L'approccio adottato per contrastare la cybercriminalità parte dalla conoscenza delle cause e dei protagonisti che compongono l'ecosistema sul quale occorre intervenire.

Internet è oggi il principale canale scelto dalla cybercriminalità per raggiungere i propri obiettivi.



La cultura dell'intelligence e il ruolo del Marketing & Competitive Intelligence

- La maggior parte delle informazioni strategiche si trova nel web e soprattutto nel **deep web** (web nascosto).
- Il mercato reale rappresenta meno del 4% dei dati utili presenti sul web.
- La conoscenza del mercato nascosto permette di avere una visione completa dell'ambiente interno ed esterno.
- Gli attori che si muovono nel web nascosto lo fanno soprattutto o per interessi ($$$) o per potere: Azioni di *market influence*, ricatti, destabilizzazione, …)

La cultura dell'intelligence e il ruolo del Marketing & Competitive Intelligence

Esistono 3 tipologie di dati sul quale bisogna concentrarsi per elaborare delle strategie di sviluppo e proteggere il proprio brand (Reputation, Risk Management & Security):

Dato o informazione pubblica

Dato o informazione sensibile

Dato o informazione Confidenziale / segreta

Etica, Legalità, Privacy ?

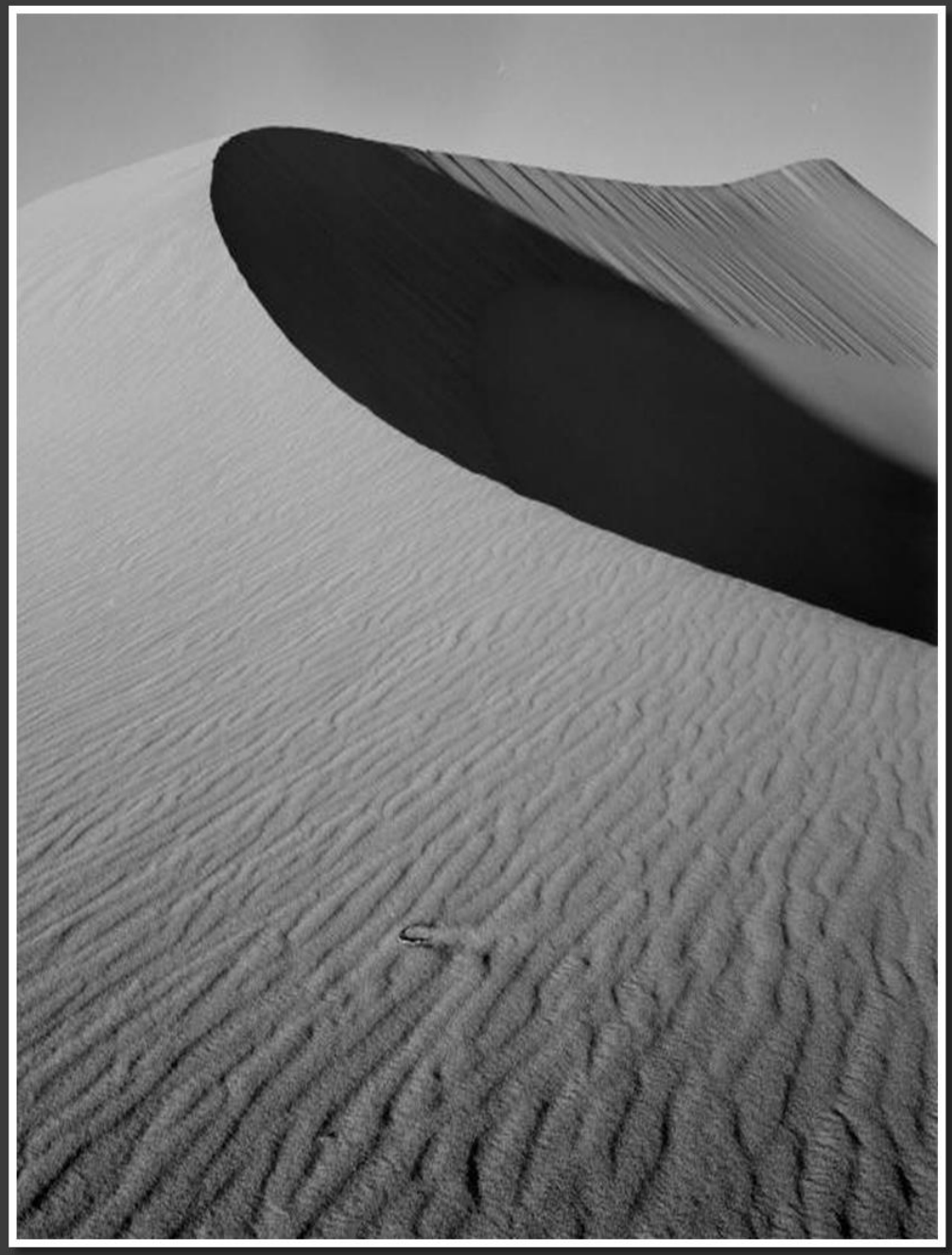
La cultura dell'intelligence e il ruolo del Marketing & Competitive Intelligence

Internet è un motore dell'economia e allo stesso momento una fonte di potere per chi lo controlla: Questo paradigma è stato compreso da numerosi paesi nel mondo ed in primis dagli Stati Uniti:

- Negli anni 90, 35 aziende americane erano classificate nel Top 50 delle aziende leader a livello mondiale nel mondo digitale
- Non a caso, l'ICAAN (*Internet Corporation for Assigned Name and Numbers*), organismo preposto alla gestione dei domini, è riconducibile ad interessi americani.

Altri paesi come la Cina, la Russia, la Korea del Nord hanno anche loro, da tempo, fatto enormi investimenti per guadagnare un posto nell'economia digitale e non solo (➔ Competitive Intelligence, Security e Controllo).

È interessante osservare oggi il comportamento dei grandi player come Apple, Facebook, Twitter, … che obbligano i loro clienti a sottostare alle condizioni dei contratti di licenza per poter usufruire dei loro servizi (*terms of service // terms of acceptance*) senza dare loro la possibilità di "negoziare"



Il dilemma delle banche

Il dilemma delle banche

Mentre gli hackers condividono le informazioni in rete …

Posted 1 Jun 2013

J'ai une grosse faille a partager sur une banque trés connus . Corb3n je t'invite a la poster :)

Membres
0
2 posts

aciD

Posted 1 Jun 2013

Faille qui permet quoi ?

You are welcome to the wonder land of hacks, want to know how to hack an ATM MACHINE OR BANK ACCOUNT?
You can hack and break into a bank's security without carrying guns or any weapon.

HOW IS THIS POSSIBLE...
Continue Reading

How to Hack a Bank Account and Atm Machine with a Free Software

August 2, 2013 ·

Check out our latest products

BUY HACKING TOOLS

Many customers have request me to give them hacking softwares and teach them hacking and thats why i write this. Here are hacking softwares i sell and price BANK HACKING ...

bank account password hacking software free download - Steganos Password Manager 16 Steganos Password Manager, and much more programs.

... a little demo on how to hack userid and password from an online Banking application. .. from the bankserver was executed, showing our account balance.

Step 5 Connect to the bank, open the HUD connection analyser and then bypass all of the security systems. Log into the account by using password hacker and ...

Il dilemma delle banche

La maggior parte delle banche fa ancora fatica a condividere le informazioni sulla Cyber Security e spesso, le notizie vengono svelate dai media o dai clienti che raccontano senza nascondersi le loro esperienze negative (citando la banca).

Le XXXXXXXXXXX, qui a déjà la fâcheuse manie de ne pas rembourser ses clients victimes de phishing, refuse de lui restituer les 2200 euros qui ont disparu de son compte.

ce qui bloque en France ,ce sont les banques françaises .Contrairement aux banques américaines elles trainent les pieds pour rembourser leurs clients victimes de fraudes (comme la XXXXXXXXX épinglée par des associations de consommateurs) .
Il faut que nos banques deviennent plus innovantes et organisées pour ne pas rater le coche du paiement via mobile.

Merci le Monde pour cet article, puisse-t'il contribuer à faire prendre conscience aux autorités, aux banques et aux victimes de ces attaques incessantes, de la nécessité de tout mettre en oeuvre pour lutter contre la cyber-criminalité et s'en protéger.

Il dilemma delle banche

Le banche sanno perfettamente che gli attachi non si fermeranno mai a causa di tutte le dinamiche in gioco come ad esempio

- Lo sviluppo delle nuove tecnologie
- il cambiamento delle abitudini dei clienti: fruizione, luoghi, dinamiche di interazione (PC/Smartphone/Tablet, Francia/estero, connessioni Wifi, …) e la loro non preparazione (conoscenza ed errori comportamentali)
- La mancanza di efficienza e di coordinamento con gli altri stati esteri

La cartografia dei punti critici di contatto sarà in continua evoluzione con l'arrivo dell'IoT (Internet of Things) e richiederà un aggiornamento sistematico delle procedure di sicurezza (➔ aumento delle APT / Advanced Persistent Threats).

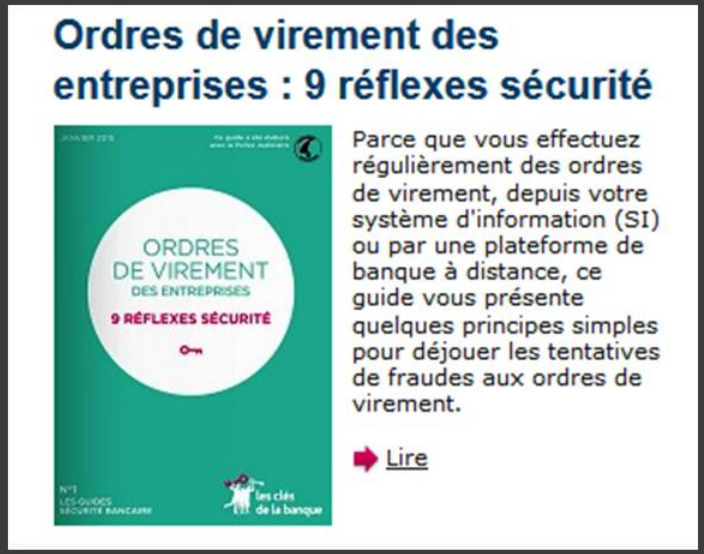
I responsabili della banca sono consapevoli del loro ruolo centrale nell'economia del paese e hanno ben chiaro questa situazione. L'unica risposta passa in primis attraverso una buona conoscenza dell'ambiente interno ed esterno (monitoring & analysis) per proteggere i loro interessi e quelli dei loro clienti.

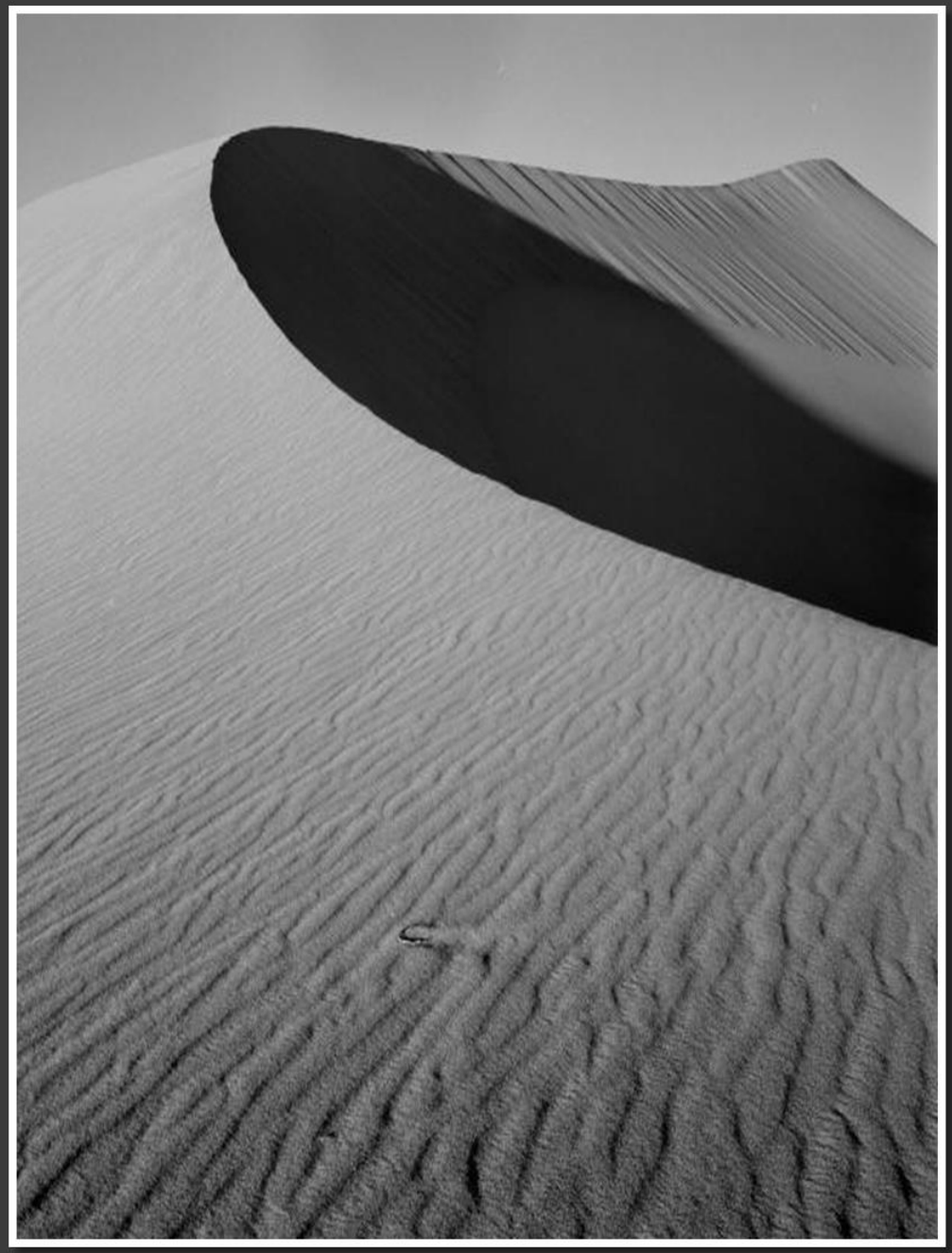
Il dilemma delle banche

Delle iniziative sono promosse dalla Banque de France e da tutti gli Istituti bancari per migliorare la loro relazione con i clienti (Informazione / Formazione e Prevenzione)

Questi incontri si svolgono su tutto il territorio e a vari livelli con diversi Player come il MEDEF (Confindustria), La Chambre des Métiers et de l'Artisanat (Confartigianato), le Camere di Commercio, … o direttamente con i dirigenti delle PMI.

Fonte: Les clés de la Banque (Fédération Bancaire Française) - 2015





L’approccio del Gruppo Bancario "X" nella gestione della Cyber Security

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

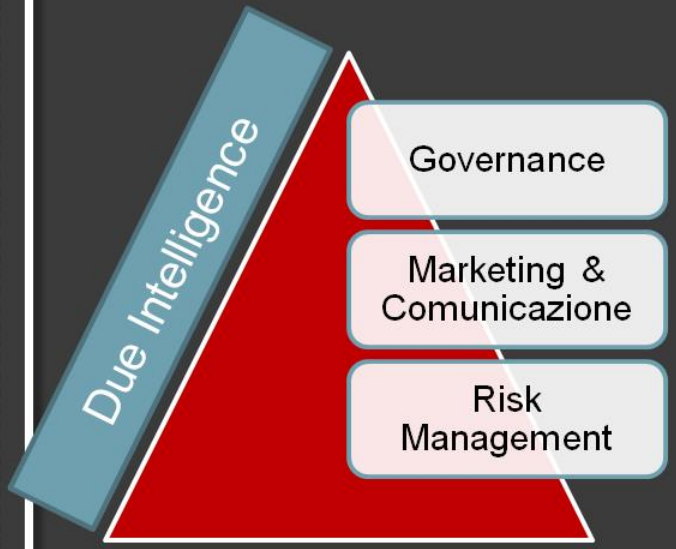
Per il Gruppo bancario, la gestione della C*yber Security* parte dalla consapevolezza dei suoi dirigenti che nessuno è al riparo e gli attacchi potrebbero colpire tutti in qualsiasi momento, creando, senza una preparazione interna adeguata, problematiche anche gravi di varie tipo.

Il *Cyber Security Risk Management* passa attraverso la conoscenza e la valutazione di informazioni pertinenti su questa tematica "evolutiva" per preparare continuamente l'intera struttura ad anticipare/rispondere in modo adeguato ad eventuali attacchi.

La *Brand Reputation* è un KPI fondamentale

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

L'attività di Marketing & Competitive Intelligence è stata programmata con lo scopo di migliorare il posizionamento competitivo della banca attraverso la conoscenza del suo ambiente interno ed esterno, prendendo seriamente in esame le tematiche della Sicurezza.



Gruppo Bancario

Data governance

Qualità
Pertinenza
Privacy
+
Capitalizzazione
(Capacità/Competenze)

- Brand leadership
- Customer experience
- Business opportunities
- Operational efficiency
- Brand protection

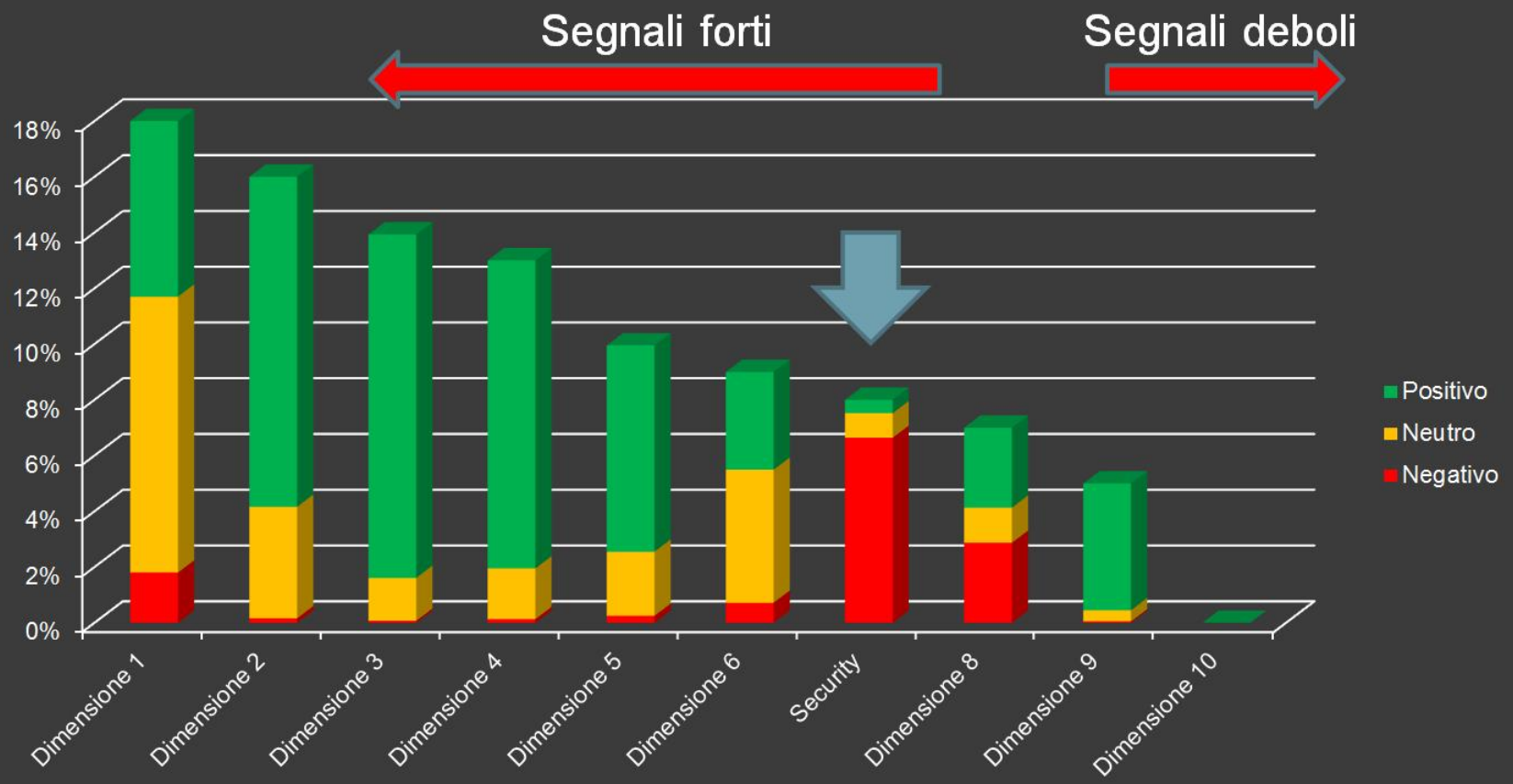
Le attività di Marketing & Competitive intelligence

- Valutazione dei risultati con impostazione di un sistema di Alert ➔ Process & Organizational Assessment
- Strategie ➔ Brand leadership + Customer Multichannel Experience + Business Opportunities + Operational Efficiency + Brand Protection (➔ fiducia da parte degli stakeholder)
- Guidelines/Best practice & Training (interno / esterno)

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

- Le attività di Marketing Intelligence hanno individuato dieci dimensioni che possono influenzare positivamente o negativamente i clienti sulla scelta della banca.
- Ogni informativa è valutata in base alla sua influenza/peso (indice DORank da 0 a 10).
- La Sicurezza è una tematica e una dimensione critica importante e il Gruppo bancario si è attrezzato per rispondere al meglio alle minacce che potrebbero colpire direttamente o indirettamente i suoi interessi (visione strategica /consapevolezza/ resilienza).

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

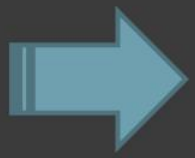


L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

Capacità/Competenze

HUMINT

Cyber Intelligence Risk Management



Data Governance & Organizational Process

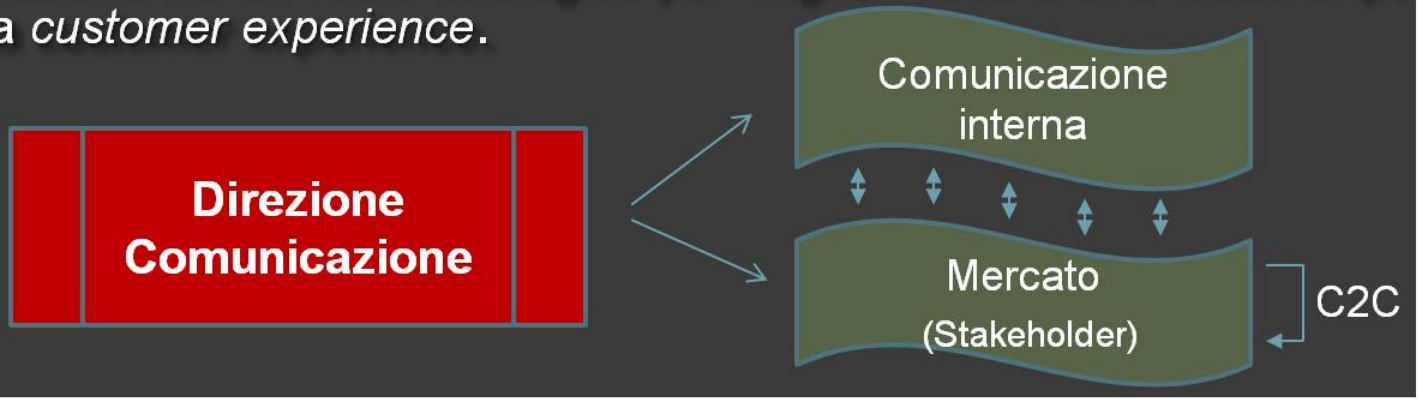
Technology (security)

Comunicazione (interna / esterna)

L'approccio del Gruppo Bancario "X" nella gestione della Cybersecurity

Il ruolo della Comunicazione

- Una relazione positiva e costruttiva tra la Banca e gli Stakeholder è un punto chiave fondamentale nella strategia commerciale della banca.
- Esiste all'interno del Gruppo Bancario un Dipartimento Antifrode che si occupa della lotta alla cyber criminalità; la sua missione consiste nel preservare gli interessi del Gruppo e dei suoi clienti a livello locale, nazionale ed internazionale. Questo gruppo di persone altamente specializzato nel campo della Cyber Security lavora con altri organismi esterni preposti alla lotta contro il cyber crime: Polizia, ANSSI, OCLCTIC, …
- La Comunicazione ha un ruolo strategico per migliorare la *brand leadership*, la *loyalty* e la *customer experience*.



L'approccio del Gruppo Bancario "X" nella gestione della Cybersecurity

Il ruolo della Comunicazione

- La Comunicazione lavora su più livelli e ha come pubblici di riferimento l'insieme degli stakeholder e il Mercato: Opinion leader, mercato finanziario, potenziali clienti, …
- Le scelte operative e gli strumenti utilizzati hanno un ruolo determinante per prevenire e abbassare i costi della Cyber criminalità. Hanno come obiettivi tutta la parte del *Brand trust*, *l'Education* e le *Best practice* (→ ad esempio per evitare gli errori comportamentali che potrebbero facilitare il lavoro dei cyber criminali)

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

Il ruolo della Comunicazione

Gli obiettivi della criminalità sono orientati sui beni finanziari. In tale senso, il Gruppo bancario

- è sensibile alla cyber security e al benessere finanziario dei suoi clienti (privati + aziende)
- desidera presentarsi come interlocutore di fiducia a tutela dei loro interessi.

➔ "Siamo qui per consigliarvi, proteggere i vostri interessi e darvi delle indicazioni" *(Nous sommes là pour vous conseiller, protéger vos intérêts et vous guider dans vos démarches)*

➔ "Il nostro Direttore e il nostro personale sapranno consigliarvi" *(Notre Directeur et notre personnel sauront vous conseiller)*.

Lo sviluppo delle nuove tecnologie e dei punti critici di contatto (➔ IoT) impongono un aggiornamento interno continuo del know-how e delle procedure (Best practice).

L'approccio del Gruppo Bancario "X" nella gestione della Cyber Security

Il ruolo della Comunicazione

La riduzione dei tempi di reazione per denunciare gli cyber attacchi è molto importante soprattutto per recuperare i soldi dei bonifici bancari.

La gestione di tutte queste situazioni delicate passa attraverso

- ➔ La conoscenza dell'ambiente: monitoring rete internet, conoscenza del mondo dell'hacking, ..
- ➔ una preparazione interna dello staff (Education & Comportamento & Organizational process)
- ➔ la programmazione di materiali ed incontri formativi con i clienti (aziende / privati)

con l'obiettivo di trasmettere ai clienti competenze, fiducia ed impegno nel risolvere i problemi.

Se conosci il nemico e conosci te stesso, nemmeno in cento battaglie ti troverai in pericolo.

Se non conosci il nemico ma conosci te stesso, le tue possibilità di vittoria sono pari a quelle di sconfitta.

Se non conosci né il nemico né te stesso, ogni battaglia significherà per te una sconfitta certa.

Sun Tzu – L'Arte della Guerra 孫子兵法

Grazie

Jamil Ouazzani
Partner Easy Business in Milan