Lo sviluppo del Presidio Antifrode in Banca

Quali modelli per gestire le nuove sfide

Paolo Colombini
Resp. Settore Security Operations Center

Roma, 06 Giugno 2013

UBI Sistemi e Servizi

Il ruolo del fraud manager

"Supportare gli sviluppi e le nuove opportunità di business sapendo gestire e mitigare i rischi"

Sviluppi

Multicanalità
Pagamenti Contactless
Mobile Banking
Mobile Payment
Remote Selling
Wallet
Mobile POS
eCommerce
…

RICAVI

- *Agevolare*
- *Favorire*
- *Supportare*

Minacce

Furto di identità
Furto di credenziali
Clonazione carte
Attacchi informatici
Malware
Phishing
…

COSTI

- *Mitigare*
- *Ridurre*
- *Gestire*

Evoluzione del presidio

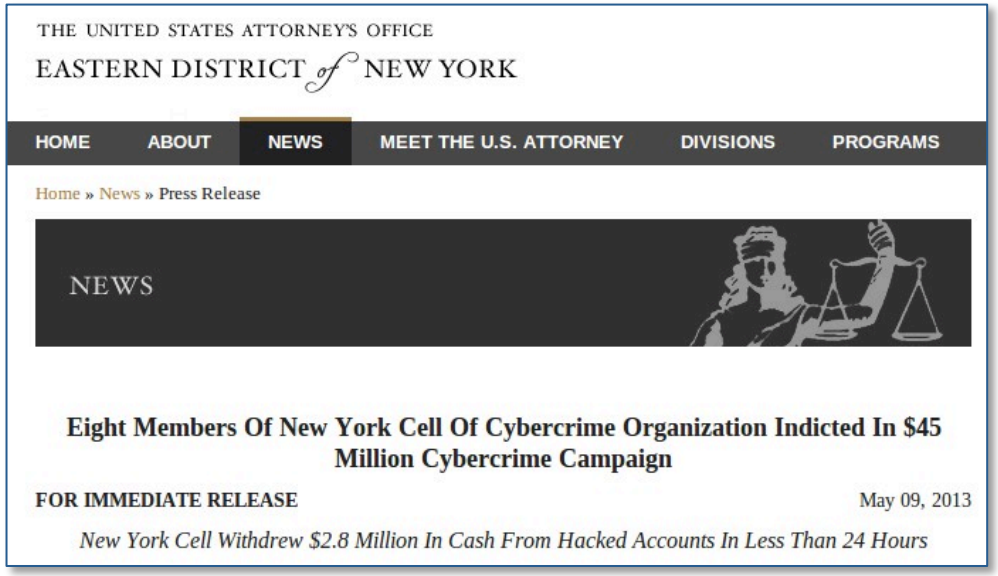
Dalla gestione tecnica al supporto ai processi di business

- Da “gestione degli strumenti“
  a “gestione dei processi *“end to end”*
- Da “gestione eventi“
  a “mitigazione dei rischi”
- Da “competenze tecniche”
  a “conoscenza degli strumenti e dei servizi di pagamento”
- Da “competenze specialistiche”
  a “comprensione dei trend di mercato”
- Da “analisi delle vulnerabilità“
  a “valutazione dei rischi dei servizi”
- Da “analisi tecnica delle misure di sicurezza”
  a “valutazione dei costi, degli impatti e della *customer experience”*

L'evoluzione delle minacce

La tempesta "quasi" perfetta

- Frode internazionale da 45M $ che ha coinvolto 27 paesi
- 45M di $ in 10 ore tramite prelievi ad ATM con carte prepagate
- Violazione di sistemi
- Furto di dati (carte)
- Alterazione limiti di prelievo
- Distribuzione mondiale dei dati delle carte rubate
- Prelievo massivo su scala mondiale



THE UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT of NEW YORK

HOME | ABOUT | NEWS | MEET THE U.S. ATTORNEY | DIVISIONS | PROGRAMS

Home » News » Press Release

NEWS

Eight Members Of New York Cell Of Cybercrime Organization Indicted In $45 Million Cybercrime Campaign

FOR IMMEDIATE RELEASE May 09, 2013

New York Cell Withdrew $2.8 Million In Cash From Hacked Accounts In Less Than 24 Hours

- Precisione "chirurgica" da parte degli hacker
- Natura globale dell'organizzazione
- Velocità e coordinamento nell'esecuzione

The "Unlimited Operation"

As alleged in the indictment and other court filings, the cyberattacks employed by the defendants and their co-conspirators in this case are known in the cyber underworld as "Unlimited Operations" – through its hacking "operation," the cybercrime organization can access virtually "unlimited" criminal proceeds.

The "Unlimited Operation" begins when the cybercrime organization hacks into the computer systems of a credit card processor, compromises prepaid debit card accounts, and essentially eliminates the withdrawal limits and account balances of those accounts. The elimination of withdrawal limits enables the participants to withdraw literally unlimited amounts of cash until the operation is shut down. "Unlimited Operations" are marked by three key characteristics: (1) the surgical precision of the hackers carrying out the cyberattack, (2) the global nature of the cybercrime organization, and (3) the speed and coordination with which the organization executes its operations on the ground. These attacks rely upon both highly sophisticated hackers and organized criminal cells whose role is to withdraw the cash as quickly as possible.

Fonte: U.S. Department of Justice
http://www.justice.gov/usao/nye/pr/2013/2013may09.html

Quali insegnamenti?

- ✓ Lo scenario di riferimento è globale e tutti possono essere coinvolti
- ✓ Attacchi informatici e frodi sono correlati
- ✓ I frodatori ragionano in modalità “multicanale”
- ✓ Il problema su un canale può diventare una frode su un altro canale/prodotto
- ✓ I frodatori gestiscono l’intero processo “*end to end*”
- ✓ I frodatori conoscono le caratteristiche peculiari di prodotti e servizi

La progettazione del Presidio Antifrode

Quanto spendere?

✓Business Case
✓Contesto

Quali servizi?

✓Multicanale
✓Multiprodotto

Quali evoluzioni?

✓Esigenze business
✓Esigenze clienti
✓Trend di settore

Quale perimetro?

✓Interno
✓Esterno

La collocazione

Business

Comprendere
Capire
Supportare

Educare
Informare
Tutelare

Clienti

Presidio Antifrode

Analisi

- *Valutazione rischi*
- *Reportistica*
- *Pareri*

Gestione

- *Verifiche*
- *Controlli*
- *Azioni*

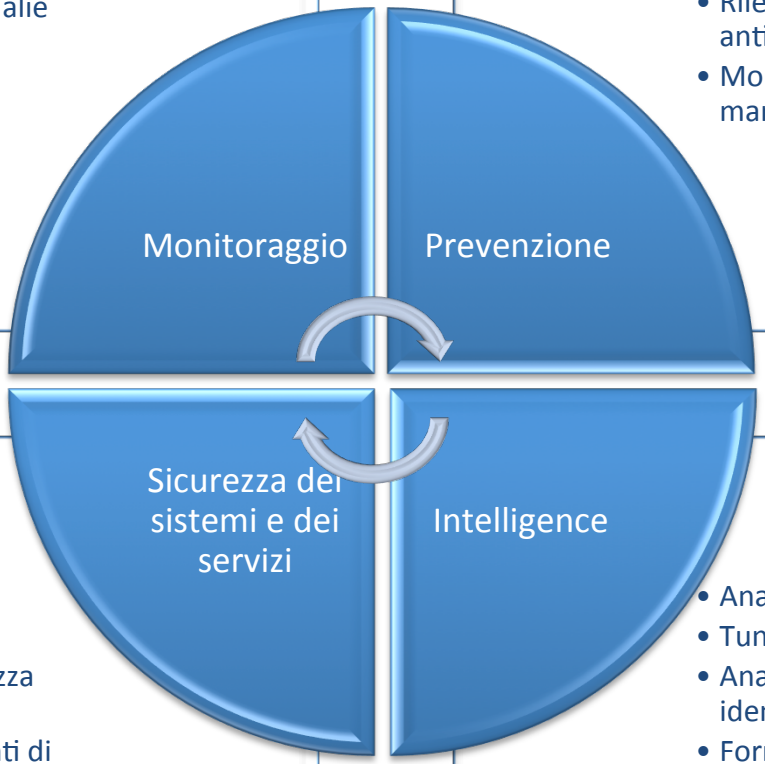
Comunicazione

- *Alert*
- *Segnalazioni*
- *Informativa*

I componenti principali del presidio antifrode

- Monitoraggio delle transazioni
- Monitoraggio degli accessi ai servizi
- Segnalazione e verifica anomalie

- Contrasto al furto di dati e credenziali (antitrojan, antiphishing)
- Rilevazione attacchi (antiphishing, antipharming)
- Monitoraggio attacchi tramite marketplace



- VA e PT continuativi
- Sicurezza delle applicazioni
- Analisi delle misure di sicurezza alla luce delle minacce
- Identificazione degli interventi di miglioramento

- Analisi periodica dei fenomeni
- Tuning dei controlli
- Analisi dinamiche frodatorie e identificazione azioni
- Formazione interna ed esterna

Fattori di successo

1. Comprensione tempestiva dei fenomeni
2. Procedure
3. Visione integrata delle minacce
4. Flessibilità e reattività
5. Networking
6. Collaborazione e relazioni con strutture aziendali
7. Relazione con i fornitori
8. Assunzione dei rischi e proattività

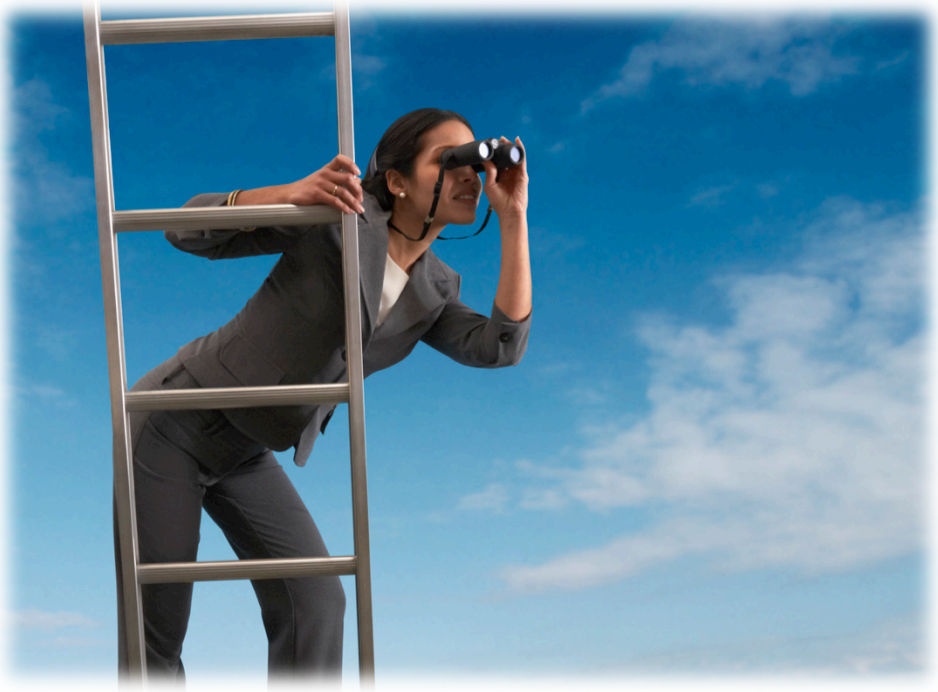
L’attenzione al cliente

- La frode ha un effetto devastante sulla percezione di sicurezza dei servizi
- Non possiamo pretendere che il cliente sia un esperto di sicurezza

CHE COSA FARE?

Prevenire	*Rendere la sicurezza “semplice”* *Prevedere i comportamenti non sicuri*
Informare	*Sensibilizzare, senza spaventare* *Spiegare i rischi ed i comportamenti da adottare*
Tutelare	*Allertare ed informare tempestivamente* *Eliminare o gestire le situazioni “rischiose”*

Che cosa attenderci?



Quali minacce?

- Attacchi mirati a vulnerabilità applicative
- Attacchi mirati al mondo mobile (lato device e lato marketplace)

Quali frodi?

- Frodi in “Multicanalità”
- Frodi di nicchia e su ambiti tradizionali

Quale contesto?

- Servizi di pagamento sempre più semplici ed integrati
- Profilazione dei clienti e distribuzione delle informazioni personali

Quali strategie adottare?

✓*Rendere la sicurezza “semplice”*
✓*Contrastare i fenomeni attuali preparandosi per quelli futuri*
✓*Monitorare costantemente le evoluzioni del mercato e le aspettative dei clienti*