REATI INFORMATICI:
LE CRITICITA' PER LE SOCIETA'

Cesare Parodi- Procura della Repubblica di Torino

Con la collaborazione del dr. Giuseppe Zuffanti- Polizia Comunicazioni Torino

La ricerca della prova: gli ostacoli strutturali

- rapida scomparsa degli elementi probatori: indispensabile una sollecita denuncia
- le tracce dell'illecita intrusione, e la possibilità di risalire all'autore del fatto reato, sono di norma legati alle capacità del soggetto "intrusore" e inoltre facilmente eliminabili
- lo stesso sistemista che ha accertato l'intrusione dopo aver verificato che non siano stati arrecati danni al sistema, provvede a "ripulire" le tracce dell'avvenuta intrusione.
- Le tracce utilizzabili contenute nei files di log del sistema possono essere cancellate dallo stesso intrusore al termine delle sue "reiterate" visite.

…la indispensabile collaborazione..

- E’ indispensabile la collaborazione dei soggetti coinvolti , ossia tra i soggetti che hanno subito l'illecita intrusione e la Polizia Giudiziaria operante
- Nessuno meglio degli operatori del sistema violato conosce la particolare architettura dello stesso, gli eventuali "bachi", le anomalie riscontrate nel tempo, le modalità di utilizzo delle password ecc.
- Questi soggetti, di norma, non conoscono le esigenze e la finalità probatorie delle informazioni in loro possesso e – per contro- la p.g. potrebbe non conoscere gli aspetti tecnici del sistema da « studiare»

Tempestività ed efficacia della denuncia

- E’ stata riscontrata una forma di "ritrosia" nei sistemisti sia di Enti Pubblici che di aziende private, nel considerare un attacco informatico come un fatto reato. Una illecita intrusione che non produce danni è normalmente tollerata e considerata una "bravata".

- Un’ illecita intrusione in un sistema, anche se non ha causato alcun danno, può essere utilizzata dall‘hacker come "ponte" per entrare in altri sistemi ove invece vengono effettuate operazioni di cancellazione dati ed altro
- NON SOTTOVALUTARE LE «INTRUSIONI»

In un caso concreto….

.

Grazie alla immediata denuncia e collaborazione del sistemista di un sistema violato si sono potuti incrociare i dati del file di log con i dati tempestivamente acquisiti presso il fornitore di accesso dell'hacker portando all'individuazione dello stesso;

- Senza la denuncia relativa al primo sistema violato – utilizzato come "ponte" per entrare in altri sistemi- questi ultimi avrebbero potuto subire gravissimi danni in quanto l'hacker aveva ottenuto l'accesso con i privilegi di root e non era stato rilevato dal sistemista ;
- Non sarebbe quindi stato possibile interrompere l'illecito utilizzo da parte dell'hacker del secondo sistema, nel quale venivano accertati successivamente danni, manomissioni e cancellazioni di dati.

I REATI INFORMATICI

Le criticità aziendali-commerciali

Le criticità del momento

COMPROMISSIONI E-MAIL DI LAVORO

Le ***BEC (Business Email Compromise)*** o le ***CEO Fraud (Chairman Executive Officer)*** : tecniche fraudolente che puntano a violare la corrispondenza intercorrente tra i rapporti commerciali fra le aziende: nel primo caso (BEC) i gruppi criminali si frappongono fra due società, sostituendosi ad una di esse, nel secondo caso (CEO Fraud), si sostituiscono a un vertice dell'azienda.

Le tecniche in argomento rientrano nel fenomeno più generale della frode informatica attraverso le tecniche del ***"Man-in-the-Middle"***, dello ***Spear Phishing*** e del ***Social Engineering***.

UN MECCANISMO CONSUETO

Un soggetto cerca di ingannare i dipendenti, ad esempio di una azienda ovvero clienti, a effettuare un trasferimento di fondi a beneficio dei truffatori stessi.

FASE 1

I dipendenti di un'azienda ricevono una mail fraudolenta, apparentemente inviata da persone o enti di cui si fidano, e che invece è mandata da truffatori; nella mail ad esempio può esserci un link o un allegato; seguendo il primo o aprendo il secondo il computer del destinatario viene infettato.

Questa è la prima fase, un attacco detto di *phishing* o meglio *spear phishing*.

…segue

FASE 2

I truffatori hanno accesso al pc e/o alla mail del dipendente. Iniziano a spiarne le comunicazioni interne ed esterne; individuano, ad esempio, i responsabili commerciali, i creditori e debitori. Si fanno un quadro della situazione e quindi arrivano alla fase tre.

Simulano, con una finta email, di essere un fornitore dell'azienda cui deve essere fatto un pagamento; e spiegano che per qualche motivo hanno cambiato Iban. **Il nuovo codice in realtà corrisponde a un conto aperto su una banca estera da un membro dell'organizzazione criminale.**

Le modalita della truffa BEC

Ad una azienda che ha un rapporto di lavoro con un fornitore da diverso tempo, viene chiesto di pagare una fattura mediante bonifico bancario.

La richiesta viene effettuata tramite telefono, fax o e-mail.

Se effettuata via e-mail verrà utilizzato un indirizzo di posta elettronica molto simile a quello originale del fornitore, se la richiesta avverrà tramite fax o telefono essa imiterà un richiesta lecita.

Le modalita della truffa BEC

- … segue

Dalla e-mail violata di un funzionario viene inviata la **richiesta di effettuare un bonifico ad un altro impiegato della medesima società che generalmente si occupa di contabilità.**

In altri casi si usa l'account di posta elettronica violato per contattare direttamente l'istituto finanziario per chiedere un trasferimento di denaro verso la banca "X" per una motivazione "Y".

…segue.

Dall’account di posta elettronica violato appartenente ad un impiegato, vengono inviate delle richieste, per evadere le fatture verso conti creati correnti creati ad hoc, a venditori presenti tra i contatti in rubrica. L’azienda può non essere consapevole delle richieste fraudolenti a meno che non venga contattata dai venditori che chiedono delucidazioni in merito alle fatture.

Le frodi di tipo BEC

Vittima: aziende che svolgono regolarmente bonifici con fornitori/terze parti estere.

Per porre in essere le truffe BEC/CEO i truffatori si servono di tecniche sia di social engineering che di spear phishing.

- **SPEAR PHISHING**
- Lo *spear phishing* è una forma di phishing mirato tramite e-mail con l'intento di ottenere l'accesso non autorizzato, ad esempio, a dati sensibili. A differenza del phishing, che sferra attacchi indiscriminati su vasta scala, lo *spear phishing* prende di mira un gruppo specifico o un'organizzazione. Ecco i passi principali:
-
- L'hacker sceglie il bersaglio, questo può essere una società che possiede informazioni utili o di cui si può ottenere l'accesso.
- L'hacker identifica un lavoratore che potrebbe aver accesso a informazioni preziose. Ne studia le abitudini sfruttando anche social network per trovare il modo migliore di indirizzare il lavoratore.

- A questo punto l’hacker invia una e-mail al dipendente preso di mira; e-mail che sembra provenire da un amico o da un collega. Spesso nell’e-mail si troverà un allegato che può sembrare normale ma che una volta eseguito consentirà l’accesso del computer all’hacker. Il codice malevolo che verrà eseguito può essere di qualità sufficiente da aggirare le difese informatiche, incluso il software antivirus.
- L’hacker utilizza il suo accesso per rubare i dati dal computer della vittima o per estrarre informazioni preziose anche grazie all’avvenuta installazione malevola di una ATP (Advanced Persistent Threat), che attende silente per poter rubare più informazioni preziose in un periodo di tempo più lungo possibile.

SOCIAL ENGINEERING

Nel campo della sicurezza informatica, il social engineering (o ingegneria sociale) è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.

Spesso, per fini criminali……

.

- Fase preliminare (foot printing)
  - Raccolta informazioni sulla vittima, indirizzi e-mail, recapiti telefonici, numeri di fax, ecc., per poi arrivare all'attacco vero e proprio.
  - La ricerca di informazioni è complessa e le fonti sono molteplici: informazioni reperite da siti web aziendali, profili di social networking, documenti pubblici…

- Fase intermedia

  - Verifica attendibilità delle fonti
  - Il s.e. cerca di entrare in contatto diretto con la “vittima” ad esempio e-mail o telefonata, cercando di entrare in sintonia dimostrando una certa sicurezza qualora vengano poste domande.

.

- <u>Fase finale (attacco vero e proprio)</u>
  - Si contatta la vittima per reperire le informazioni desiderate (richiesta di username e password causa controlli sulla casella di posta elettronica, assistenza remota, ecc.).
    - Il tutto viene condotto con tono molto accomodante e convincente al fine di spingere l'interlocutore a fornire le informazioni richieste.
    - Es: una breccia nel sistema informatico della vittima per violare la rete aziendale

.

Le conseguenze penali:
la qualificazione delle condotte

IL “ CAMMUFFAMENTO” BANCARIO

del reato di cui agli artt. 648 bis c p., in quanto riceveva sul conto IBAN …… intestato a…..

un bonifico on line dell’importo di Euro …..

denaro provento illecito dei delitti di cui agli artt. 615 ter, 640 ter, 615 quinquies c.p. c.p. ad opera di ignoti (in particolare la somma sopra indicata, destinata a XXX da parte di un cliente di estero- YYY- quale pagamento di una fornitura veniva da quest’ultimo trasmesso a mezzo di bonifico on line al coordinate bancarie sopra indicate, non corrispondenti a XXX in quanto con una mail apparentemente riferibile a quest’ultima, installata a mezzo di programma cd “virus” venivano comunicate le coordinate bancarie fittizie di cui sopra), in modo da ostacolare l’identificazione della provenienza delittuosa dello stesso.

CONCORRENZA SLEALE CON VALENZA PENALE

del reato di cui all'art. 615 ter, 1° e 2° co. n 1 c.p., per avere, con più azioni esecutive di un medesimo disegno criminoso ex art 81 cpv cp, posto in essere **accessi abusivi al sistema informatico protetto da misura di sicurezza** di XXX

finalizzati a visionare ed acquisire **dati ed informazioni commerciali dal sistema informatico di proprietà della società sopra indicata**; in particolare per avere effettuato accesso abusivi al sistema, visionando ….. pagine , per un tempo complessivo di h …….,. consultando ordini e contatti con clienti della società;

con l'aggravante di aver effettuato gli accessi con abuso della qualità di operatore di sistema, avendo utilizzato, anche dopo la cessazione del rapporto di collaborazioni con XXX, account rilasciati nell'ambito di tale rapporto e con l'aggravante ex art 61 n 2 cp. di aver commesso il fatto per commettere il reato infra precisato

…segue:

del reato di cui all'art. 640 ter , 1° e 2° co, c.p. in quanto , intervenendo senza diritto sul sistema informatico di XXX- con più azioni esecutive di un medesimo disegno criminoso ex art 81 cpv cp , con le modalità ed i tempi di cui al capo precedente- si **procuravano il profitto costituito dalla disponibilità dei dati ed informazione duplicati dal sistema stesso, funzionali ed in concreto finalizzati all'utilizzo** nell'ambito dell'attività di KKK - concorrenziale rispetto a quella di XXX - ed in effetti rinvenuti in parte su supporti memoria di massa riferibili a KKK (in particolare tra l'altro budget, rendiconti, presentazioni aziendali, contratti, offerte , ordini, liste clienti, fatture, listini prezzi), impiegando informazioni riferibili a XXX **per implementare banche dati di KKK, analizzare la profilazione dei clienti, ad effettuare valutazioni economico commerciali e comune funzionali all'attività di impresa di quest'ultima società**;

Con l'aggravante di aver effettuato gli accessi con abuso della qualità di operatore di sistema, avendo utilizzato, anche dopo la cessazione del rapporto di collaborazioni con XXX, account rilasciati nell'ambito di tale rapporto

CONCORRENZA CON DANNEGGIAMENTO

del reato di cui all'art. **635 quater c.p. commi 1, 2 in relazione all'art. 635 bis c.p**, per avere restituito a XXX, un notebook di proprietà di quest'ultima società che lo stesso aveva in uso, previa formattazione, in tal modo rimuovendo tutti i dati, le informazioni aziendali e i programmi gestite e implementate dalla stesso ….. (che operava quale impiegato tecnico di IV livelle da dieci anni incaricato di gestire il sistema informatico dalla società) che si trovavano memorizzate, in via esclusiva, sullo stesso; di modo che la cancellazione dei dati, informazioni e programmi aziendali determinava **una temporanea compromissione della funzionalità del sistema ostacolandone gravemente il funzionamento**; con l'aggravante di aver commesso il fatto con abuso della qualità di operatore di sistema.

…segue:

del reato di cui agli art 61 n 11, 646 c.p. cp per essersi appropriato, al fine di procurare a se un ingiusto profitto , **dei documenti informatici contenenti dati, informazioni aziendali e programmi gestite e implementate nell'ambito della propria attività di impiegato tecnico incaricato di gestire il sistema informatico** di XXX, dei quali aveva il possesso in quanto memorizzati sul notebook di cui al capo precedente, duplicandoli prima della formattazione sopra descritta;

con l' aggravante di aver commesso il fatto con abuso di prestazione d'opera, avendo agito nella qualità sopra indicata.

LA FRODE INFORMATICA “CONTABILE”

Del reato di cui all’art. 640 ter , 1° co., c.p, per avere posto in essere con più azioni esecutive di un medesimo disegno criminoso ex art 81 cpv. c.p.,un intervento senza diritto sul sistema informatico della società XXX; in particolare per avere:

- - nel caso di acquisti di merce con versamento della somma mediante carta di credito, **omesso di emettere lo scontrino fiscale evitando altresì di aggiornare il quantitativo di capi presenti in magazzino** (al fine di eludere la tracciabilità del capo di vestiario e di poter sottrarre in contanti la somma di denaro, appena addebitata al cliente con l’operazione pos “effettuata”, dal registratore di cassa “sostituendola” con lo scontrino dell’operazione pos di cui sopra.)
- - intervenendo quindi sul sistema informatico del punto vendita **modificando i dati contenuti nello stesso, rideterminando le somme risultanti dalle vendite, alterando i dati informatici** che riportavano le operazioni contabili indicate con la lettera “p” (operazioni con carte di credito/debito) con la lettera “c” (operazioni contanti);
- con l’aggravante di aver commesso il fatto con abuso della qualità di operatore di sistema e- ex art 61 n 2 c.p. - per assicurarsi l’impunità del reato sub b).

…segue:

Del reato di cui all'art. 624 c.p., per essersi impossessato, con più azioni esecutive di un medesimo disegno criminoso ex art 81 cpv. c.p. , della somma complessiva di Euro ……, di proprietà della società sopra indicata, delle quale aveva la detenzione nella sua qualità di addetto all'incasso all'atto dei capi in vendita;

con l'aggravante di aver commesso il fatto con abuso di prestazione d'opera.

VENDITE ON LINE

In relazione al reato di truffa commesso attraverso vendite “on line”, la S.C. (Cass., Sez. II. dep. 14/10/1016, n. 43705) ha ritenuto configurabile la circostanza aggravante della c.d. minorata difesa, prevista dall’art. 61 n. 5 cod. pen., richiamata dall’art. 640, comma 2, n. 2 bis, cod. pen.; una soluzione per molti aspetti condivisibile, che tuttavia deve essere verificata nel caso concreto e che impone riflessioni anche legate alle modalità del fatto e all’impatto dello stesso sulle persone offese dello stesso.

- *“per avere profittato di circostanze di luogo e di tempo tali da ostacolare la privata difesa, avendo commesso il fatto attraverso contatti telematici e a distanza che non permettono alla persona offesa di controllare l'identità e la serietà dell'interlocutore/contraente, né l'esistenza del bene offerto".*
-
-

SEMPRE APPLICABILE ?

LE REGOLE SULLA COMPETENZA

I REATI "PATRIMONIALI"- l'art. 640 ter

- *Sez.* 6, *n.* 3065 *del* 04/10/1999 Cc. (dep. 14/12/1999) Rv. 214942

Il reato di frode informatica (art. 640 ter cod. pen.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. **Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui**.

Il luogo deve intendersi quello ove è stato aperto il conto o attivata la carta sul quale è stato conseguito il profitto

IL “FENOMENO” E-BAY

Non viene inviato l’oggetto pagato

Se non sussistono specifici elementi di sospetto:

inadempimento civilistico.

Obbligo di iscrizione del beneficiario dell’accredito per il solo fatto della ricezione del pagamento ?

E il beneficiario di un pagamento effettuato con carta di credito indebitamente utilizzata ?

Ipotesi: sarebbe accolta una richiesta di assistenza internazionale sulla base di tale solo elemento?

L’uso indebito di carte on line

- Cass., *Sez.* 2, *n.* 17748 *del* 15/04/2011 Ud. (dep. 06/05/2011) Rv. 250113:

Integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua.

- Analogamente Cass. Pen., Sez. II, Sent. 10.01/28.03.2012 n° 11699

- *Sez.* 5, *n.* 2672 *del* 19/12/2003 Cc. (dep. 27/01/2004) Rv. 227816

- Il delitto di **accesso abusivo** a un sistema informatico previsto dall'art. 615-ter cod. pen. può concorrere con quello di **frode informatica** di cui all'art. 640-ter cod. pen., in quanto si tratta di reati diversi: la frode informatica postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del reato di accesso abusivo che, invece, può essere commesso solo con riferimento a sistemi protetti, requisito non richiesto per la frode informatica.

PISHING- 640 ter e 615 quater c.p.?

L'operazione può avvenire tramite server stranieri.

Una mail segnala improbabili controlli o vincite e induce ad entrare nel sito della Banca o delle Poste e reindirizza su un server straniero clone di quello ufficiale, dove viene chiesto di digitare le proprie credenziali.

Concorso tra art. 640 ter e 615 quater c.p. ?

IL “FENOMENO” E-BAY …. ancora

Attività poste in essere presentandosi:

- con un account “ falso”
- con un account “rubato”

Il “furto” di identità potrebbe risalire a molto tempo prima dell’utilizzo dell’account : PROBLEMI di PROVA…. su acquisizione dei log

IN CONCRETO….

Il soggetto che ha violato un p.c. e comunque acquisito o generato i dati di una carta NON coincide con il beneficiario dell'utilizzo

Di cosa risponde il beneficario?

- ricettazione ?
- incauto acquisto ?
- concorso nell'art. 640 ter c.p. ?

Problemi di prova dell'elemento soggettivo

E' indispensabile iscrivere il beneficiario ???

IL RICICLAGGIO

Dopo l'acquisizione dei dati di un conto/ carta on line, viene richiesto a terzi di "girare" su conti esteri somme trasmesse per via telematica, a fronte di una commissione

- Buona fede del terzo?
- Se NON è credibile, il reato si consuma nel luogo ove tale soggetto "pulisce" la somma disponendo un bonifico all'estero.

Art. 648 bis c.p.

I DATI PERSONALI

***Sez.* 3, *n.* 5728 17/11/2004 (dep. 15/02/2005) Rv. 230834**

Il trattamento dei dati personali, che non siano sensibili né abbiano carattere giudiziario, effettuato da un soggetto privato per fini esclusivamente personali è soggetto alle disposizioni del d.lgs 196/2003 solo **se i dati siano destinati ad una comunicazione sistematica o alla diffusione ed è in tal caso subordinato al consenso dell'interessato**, a meno che il trattamento riguardi dati provenienti da pubblici registri od elenchi conoscibili da chiunque.

Aver comunicato ad alcuni "provider" le generalità, l'indirizzo, ivi compreso quello di posta elettronica, il numero di telefono e il codice fiscale di una persona senza il suo consenso, al fine di aprire un sito internet e tre nuovi indirizzi di posta elettronica a nome di tale persona, **non integra il reato di cui all'art. 167, co. 1 D.Lgs. n. 196/2003.**

Grazie