MEF Dipartimento del Tesoro

Newsletter

Frauds: some facts

DIREZIONE V:
Prevenzione dell'Utilizzo del Sistema Finanziario per Fini Illegali

UFFICIO VI

Newsletter n° 16 - Luglio 2017

In questo numero:

MONDO CYBER: I lavori di G7 in ambito finanziario

Nell'estate 2015 i Deputies G7, concordando sulla necessità di rafforzare la sicurezza cibernetica nel settore finanziario, date le significative interconnessioni esistenti e i conseguenti rischi di contagio, hanno deciso di costituire un gruppo di lavoro di esperti in materia (G7 Cyber Expert Group, G7-CEG).

Il mandato del gruppo è stato quello di rafforzare la cooperazione tra i sette in materia e di identificare i rischi cibernetici nel settore finanziario attraverso un esercizio di *stock-taking*, basato sui risultati di una *survey* che guardava ai ruoli, alle competenze e alle responsabilità delle varie autorità nazionali, agli approcci adottati, alle procedure per prevenire gli attacchi e per mitigare i rischi.

Il G7-CEG si è riunito varie volte nel tempo per discutere: i) di eventuali aggiornamenti sulle ultime modifiche normative e di *policy* in materia di Cyber Security del settore finanziario; ii) della guida in corso di approvazione di Cyber Resilience di CPMI-IOSCO; iii) dei risultati della *survey*.

Alla riunione dei Ministri e Governatori G7 di Sendai nel maggio 2016 è stato presentato il rapporto del gruppo in cui si evidenziavano le carenze in termini di Cyber Security riscontrate nei paesi G7. Il rapporto sintetizzava i risultati della *survey* effettuata nel mese di febbraio e articolata su quattro parti: 1) gli attori istituzionali coinvolti; 2) gli strumenti regolatori e statutari legati alla sicurezza cibernetica nel settore finanziario; 3) il coordinamento e lo scambio di informazioni; 4) la stabilità finanziaria e le infrastrutture critiche. Sono poi state formulate quattro raccomandazioni. La prima prevedeva l'individuazione, entro ottobre 2016, di un set di elementi fondamentali, non legalmente vincolanti (una sorta di *best practices* molto generali).

Agli Annual Meetings di Washington (ottobre 2016) è stato approvato dai Ministri e Governatori il set di elementi fondamentali, non legalmente vincolanti e ne sono stati individuati otto: i) strategia e *framework*; ii) *governance*; iii) valutazione del rischio del sistema dei controlli; iv) monitoraggio continuo; v) *information sharing*; vi) *response*; vii) *recovery*; viii) *continuous learning*.

Sotto presidenza italiana i *Terms of Reference* del mandato sono stati poi rivisti, principalmente al fine di estendere i G7 Fundamental Elements of Cybersecurity anche a paesi non G-7 e sviluppare principi/*basic elements* sulla seconda raccomandazione del Rapporto di Sendai, inerente, però, l'efficacia del *cyber assessment*. Si é, inoltre, affermata l'idea di incoraggiare il coordinamento internazionale e la condivisione delle conoscenze sul tema, condividendo l'idea che

il gruppo G7 CEG potrebbe fungere da cabina di regia, nonché di esaminare altri temi d'interesse su indicazione dei Deputies G7, tra cui la raccolta di dati affidabili ed omogenei, al fine di migliorare la valutazione del rischio cibernetico per l'economia reale.

Anche la Presidenza tedesca ha inserito nell'agenda del G20 il tema della sicurezza

cibernetica con un esercizio di *stock-tacking* (da affidare al FSB) simile a quello effettuato in ambito G7, cui aggiungere una dichiarazione più politica sulla rilevanza della Cyber Security e un impegno dei venti a preservarla.

MONDO CYBER: I lavori di G7 in ambito Esteri

a cura dell'Ing. Pierluigi Paganini

I recenti rapporti delle agenzie di intelligence e delle principali aziende di sicurezza confermano un incremento nel numero di attacchi cibernetici, ma ancor più preoccupante è il livello di complessità sempre più elevato. Ecco, quindi, che ci si trova a discutere del cyber spazio equiparandolo ad una "global commodity" di vitale importanza per l'attuale società tecnologica.

Il gruppo di lavoro Cyber G7 è riuscito ad ottenere il consenso degli altri membri circa la Dichiarazione sul comportamento responsabile degli Stati nel cyber spazio. Indicazioni circa la condivisione degli intenti esposti nella dichiarazione erano pervenute a seguito della approvazione della Dichiarazione nel corso del G7 Esteri tenutosi a Lucca.

Il punto 7 del comunicato finale del Summit G7 di Taormina riconosce proprio la necessità di approfondire gli argomenti esposti nella Dichiarazione al fine di garantire la sicurezza dei cittadini in un contesto globale di stabilità.

La Dichiarazione è un passo avanti nella definizione e condivisione di regole di comportamento tra stati nel cyberspazio, regole ritenute necessarie per fronteggiare le crescenti minacce cibernetiche portate da diverse categorie di attori "ostili" ai cittadini, alle imprese, ed agli Stati stessi. Gruppi di cyber criminali, attori nation-state, attivisti e terroristi rappresentano, infatti, una minaccia per ciascuno Stato, da qui l'urgenza di disciplinare l'operato degli stessi nel cyber spazio.

Ad aggravare la situazione è la totale assenza di regole e l'oggettiva difficoltà di attribuzione di un attacco cibernetico e, proprio per tale ragione, servono regole condivise che fungano da deterrente per qualunque abuso del cyber spazio e delle strutture ad esso afferenti.

Da qui l'importanza della Dichiarazione nel promuovere la cooperazione tra Stati, la condivisione di informazioni, attribuendo a ciascun membro precise responsabilità per l'implementazione di misure atte a contenere le minacce cibernetiche.

Nell'attuale scenario cibernetico, la collaborazione tra le nazioni è un requisito indispensabile ad agevolare l'attribuzione di un attacco e l'identificazione dell'azione di un attore malevolo, ecco perché i l G7 vuole e deve essere anche un momento di confronto tra le diverse strategie in materia di cyber security.

FOCUS: Speciale BITCOIN

"Il Bitcoin e le sue evoluzioni verso l'anonimato, riflessioni tecniche e giuridiche"

Introduzione

Il protocollo Bitcoin è tristemente noto per il suo utilizzo nell'ambito del dark web, del riciclaggio e della compravendita di merce illegale. Il motivo di questa diffusione è la caratteristica di anonimato – o in realtà "pseudo" anonimato – del protocollo, che comporta per gli investigatori una certa difficoltà nell'associare gli indirizzi, i wallet e le transazioni con la reale identità degli utilizzatori.

La realtà è che il Bitcoin è un protocollo basato su un registro pubblico delle transazioni, una sorta di "estratto conto" di tutti i trasferimenti di moneta virtuale avvenuti a partire dal 2009, anno del lancio del protocollo. Chiunque è quindi in grado di visionare qualunque transazione avendo contezza dell'indirizzo Bitcoin del mittente e del ricevente (in realtà possono esserci più indirizzi mittenti e riceventi), oltre che l'importo. Tramite tecniche di Bitcoin intelligence si può poi cercare d'identificare la corrispondenza tra identità e indirizzi e persino raggruppare tra di loro più indirizzi, ricostruendo i wallet all'interno dei quali sono stati inseriti. Grazie allo studio della transazione di un utente, quindi, è possibile risalire alle altre eseguite dallo stesso utente e ricostruire il suo insieme d'indirizzi bitcoin. L'analisi della rete, poi, può persino portare a identificare, in tempo reale e in alcuni casi specifici, gli indirizzi IP degli utenti che hanno eseguito transazioni, permettendo d'identificare l'utenza stessa dalla quale sono avvenute le operazioni di trasferimento. Ovviamente anche con il Bitcoin è possibile adottare contromisure per nascondere la propria identità, utilizzando Mixer e Tumbler oppure operando da wallet online o con client Bitcoin connessi dietro la rete anonima Tor.

Viene quindi a cadere quell'alone di anonimato che circonda il Bitcoin che diventa, paradossalmente, una moneta tra le più controllabili e trasparenti. In particolare, quando la trasparenza si lega con un'attività di cash-out durante la quale all'anonimato non è stata data la giusta attenzione, il cerchio si può chiudere e l'identificazione di una delle due controparti diventa possibile.

Si apre quindi la strada a nuove monete digitali che fanno dell'anonimato la base di funzionamento e non una *feature* aggiuntiva e integrabile.

Le monete a zero knowledge

Sul sito della nuova moneta Zcash (ZEC) viene subito chiarita la differenza con il Bitcoin: pur condividendo un registro delle transazioni decentralizzato e pubblico, il nuovo protocollo nasconde, per ogni transazione, il mittente, il destinatario e l'importo. Coloro che possono visionare questi dati sono il destinatario stesso o eventuali altri utenti autorizzati. Dal punto di vista tecnico, le Zcash, tramite un protocollo che utilizza una prova definita a *zero-knowledge,* cifrano il contenuto

delle transazioni protette ma permettono al sistema di mantenere in modo sicuro i corrispettivi di ogni indirizzo, senza con questo permettere agli utenti di conoscere questa informazione. Lo stato di avanzamento del progetto non è ancora tale da renderlo diffuso, per utilizzare la moneta è necessario installare un programma per Linux senza interfaccia grafica, quindi destinato per ora ai più esperti.

Alternativa a Zcash, Monero (XMR) si focalizza su privacy, decentralizzazione e stabilità, basando il suo funzionamento sul protocollo CryptoNote che garantisce l'anonimato delle transazioni e degli indirizzi. Più diffuso del gemello Zcash, Monero è noto ai più perché è stato adottato dal black market Alphabay che, nel dark web, permette la compravendita di merce illegale garantendo l'anonimato di acquirenti e venditori.

Tramite protocolli *zero-knowledge* come ZEC e XMR è possibile rendere la fase di cash-out più difficile da identificare, conferendo nuovamente importanza agli strumenti investigativi tradizionali (la Computer e Network Forensics può inserirsi fra essi), che possono apportare valore aggiunto a quelli tecnologici.

Entrambi i protocolli sono recenti, non si esclude quindi che – con ulteriore ricerca – si possa arrivare più avanti a ridurne l'anonimato, così come è avvenuto con il Bitcoin, per il quale ormai esistono società che a pagamento forniscono informazioni sui wallet, sugli indirizzi e le transazioni e persino strumenti gratuiti che, con minore affidabilità, riescono a identificare il wallet da cui proviene un indirizzo (in particolare se si tratta di un exchange, sito di gioco, etc…) e, talvolta, a fornire informazioni utili per eventuali indagini.

Aspetti Economici

La tecnologia e le innovazioni portate dallo pseudonimo Satoshi Nakamoto hanno cambiato la prospettiva, le tendenze e le evoluzioni. Per la prima volta è stato realizzato un sistema umano autonomo, che diventa inarrestabile, con un'unità di conto la cui natura giuridica è un vero grattacapo.

L'unica pronuncia ufficiale è costituita dalla Sentenza della Corte di Giustizia dell'Unione Europea nel caso C-264/14 (Hedqvist) in cui, pur affrontando i profili IVA, è stato sottolineato come le valute virtuali non sono e non possono essere né consumate, né utilizzate come beni, ma esclusivamente per la funzione propria.

In tale prospettiva i mezzi di pagamento non hanno alcun'altra possibilità pratica d'impiego se non quella di un mezzo di pagamento, dato che la loro funzione si limita, con riguardo ad un'operazione, a rendere più agevole lo scambio di beni all'interno di un sistema economico. I bitcoin quindi sono considerabili quali mezzi di pagamento semplici la cui funzione si esaurisce in se stessa.

Un mezzo di pagamento richiede, però, che l'unità di conto, l'unità di misura sia perfettamente fungibile, vale a dire che non sia possibile scegliere se accettarla o meno in ragione della sua provenienza, pena la dissoluzione del sistema dato che, in tale caso, sarebbe possibile discriminare una unità di conto piuttosto che

un'altra. Analizzata da un diverso punto di vista, solo l'ultima provenienza (wallet) o l'utente che invia la transazione può determinare il discrimine, ma non certamente l'unità di conto o le modalità in cui è pervenuta. Il sistema deve, quindi, permettere che tutte le unità di conto abbiano eguale valore a pena di disgregazione.

Il protocollo Bitcoin contiene in sé il rischio potenziale della tracciabilità con riduzione della fungibilità dell'unità di conto: la tendenza del settore cerca di aumentare la fungibilità attraverso la diminuzione delle informazioni pubbliche.

Dall'altro lato, la potenzialità delle valute virtuali nel trasferimento di valore ha interessato autorità legislative e governative per analizzarne gli schemi e valutarne rischi e vantaggi.

Aspetti Giuridici

L'analisi sui rischi in Europa è iniziata il 20.11.2015 durante la riunione del Consiglio di Europa "Giustizia e affari interni" in seguito ai tragici attacchi terroristici di Parigi, con la richiesta alla Commissione di presentare proposte per rafforzare, armonizzare e migliorare i poteri delle unità di informazione finanziaria (UIF) e la reciproca cooperazione, segnatamente attraverso l'adeguata integrazione della rete di scambio di informazioni FIU.NET in seno ad Europol. Tra le altre misure veniva richiesto di rafforzare i controlli sui metodi di pagamento non bancari, quali pagamenti elettronici/anonimi, rimesse di denaro, portavalori, valute virtuali, trasferimenti di oro o metalli preziosi e carte prepagate, in linea con il rischio che costituiscono.

Il Parlamento Europeo e la Commissione Europea hanno svolte le proprie analisi e approfondito i vari schemi di valuta virtuali giungendo rispettivamente alla Risoluzione del Maggio 2016 e alla proposta di modifica della IV direttiva antiriciclaggio (2015(849)UE) del Luglio 2016.

In estrema sintesi, il Parlamento Europeo sottolinea, che, pur sussistendo la possibilità che le valute virtuali siano utilizzate per finanziare attività terroristiche, recentemente (il 18 gennaio 2016) Europol non ha confermato, in base alle informazioni possedute dalle autorità, l'utilizzo delle valute anonime per finanziare attività terroristiche.

La Commissione ha proposto un testo che identifica alcuni attori qualificati, cui demandare l'applicazione dei presidi antiriciclaggio, per rintracciare e identificare il contatto tra valute a corso legale e valute virtuali sulla base del principio di proporzionalità e la necessità di evitare di costituire un freno all'innovazione.

I soggetti individuati cui estendere gli obblighi di identificazione e segnalazione sono gli Exchanger (fornitori di servizi di scambio tra le valute virtuali e valute fiat) e i fornitori di wallet di custodia per le valute virtuali. La proposta cerca di dare chiare definizioni per avere un linguaggio comune. Le valute virtuali sono definite "*una rappresentazione digitale di valore che non viene emesso da una banca centrale o da un'autorità pubblica e non necessariamente collegato a una moneta a corso legale, ma è accettato da persone fisiche o giuridiche come mezzo di pagamento e può essere trasferito, immagazzinato o scambiato elettronicamente*".

Le definizioni sono in corso di discussione ma è proposto di attrarre quali soggetti destinatari gli Exchangers quali "*prestatori di servizi impegnati principalmente e*

professionalmente nel settore dei servizi di cambio tra valute virtuali e valute fiat". Nelle note esplicativa la Commissione mette in evidenza tuttavia che: "*L'inclusione di piattaforme di Exchanger virtuali e di fornitori di Wallet di custodia non risolverà totalmente la questione dell'anonimato collegato alle operazioni in valuta virtuale, dato che grande parte dell'ambiente delle valute virtuali rimarrà anonimo perché gli utenti possono anche effettuare transazioni senza utilizzare piattaforme di exchanger o di prestatori di wallet di custodia*".

Conclusioni

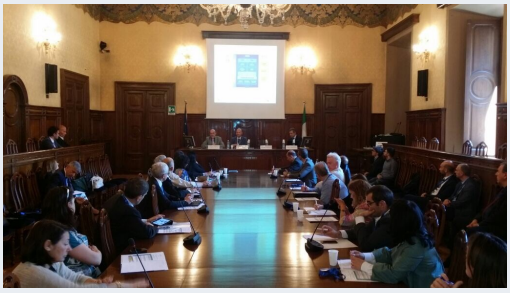
I sistemi di valuta virtuale e i protocolli delle criptovalute pongono sfide inimmaginabili che necessitano di risposte che tengano in considerazione lo sviluppo tecnologico e la tendenza alla decentralizzazione e disintermediazione in corso.

Il Bitcoin è la dimostrazione di come un protocollo che tradizionalmente è stato identificato come "anonimo" permette invece di tracciare, sotto alcune condizioni, informazioni strategiche al punto che è nata la necessità di generare due nuove monete matematiche, Monero e Zcash. Monete queste con un grado di anonimato già in fase di progetto superiore a quanto garantito dal Bitcoin, ma ancora troppo recenti per poter confermare tale caratteristica, che potrebbe essere ridimensionata da studi futuri.

Paolo Dal Checco svolge attività di Consulenza Tecnica in ambito forense. E' socio fondatore dello studio di consulenza informatica forense "Digital Forensics Bureau" di Torino. Professore a Contratto del corso di Sicurezza Informatica per l'Università degli Studi di Torino, nel C.d.L. in Scienze Strategiche, socio IISFA, CLUSIT, AIP e Tech & Law, è tra i fondatori dell'Osservatorio Nazionale per l'Informatica Forense e dell'Associazione DEFT. Da alcuni anni s'interessa d'indagini sui ransomware e degli aspetti tecnici e investigativi del protocollo Bitcoin, contribuendo ad attività di formazione per Forze dell'Ordine e di supporto all'Autorità Giudiziaria.

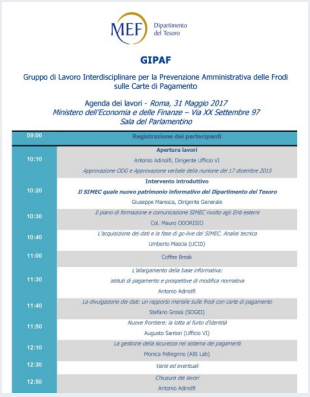
Stefano Capaccioli svolge la professione di Dottore Commercialista e Revisore Legale in Arezzo dal 1997. Cultore di Informatica Giuridica alla Università Statale di Milano, fondatore e componente del consiglio direttivo di Assob.it, fondatore di Coinlex, socio IISFA e dell'Associazione Difensori Tributari. Tra i primi ad avvicinarsi al fenomeno bitcoin e criptovalute, sviluppando teorie e interpretazioni innovative sfociate in una monografia "*Criptovalute e bitcoin: Un'analisi Giuridica*", Giuffré Editore, 2015, nonché di oltre 16 saggi scientifici e 30 articoli su varie riviste principalmente su bitcoin e metalli preziosi.

UN GIPAF ALL'INSEGNA DEL SIMEC
"Prevista per il 18 settembre la fase di go-live del nuovo applicativo"



Si è tenuta il 31 maggio a Roma presso la Sala del Parlamentino del Ministero dell'Economia e delle Finanze la riunione del Gipaf, il Gruppo Interdisciplinare per la Prevenzione Amministrativa delle Frodi.

Il Gruppo di lavoro è composto da esperti in materia di carte di pagamento ed è formato da rappresentanti del MEF, del Ministero dell'interno, del Ministero della Giustizia, del MISE, oltre che da rappresentanti della Banca d'Italia, delle Forze di polizia, dell'ABI e delle società segnalanti che emettono carte di pagamento e ne gestiscono le relative reti commerciali. Argomento centrale dell'iniziativa è stato il SIMEC, quale nuovo patrimonio informativo del Dipartimento del Tesoro nell'acquisizione, gestione, elaborazione e valutazione dei dati utili alla prevenzione amministrativa delle frodi.



MEF Dipartimento del Tesoro

GIPAF

Gruppo di Lavoro Interdisciplinare per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento

Agenda dei lavori - *Roma, 31 Maggio 2017*
Ministero dell'Economia e delle Finanze – Via XX Settembre 97
Sala del Parlamentino

09:00	Registrazione dei partecipanti
10:00	Apertura lavori Antonio Adinolfi, Dirigente Ufficio VI *Approvazione ODG e Approvazione verbale della riunione del 17 dicembre 2015*
10:20	Intervento introduttivo ***Il SIMEC quale nuovo patrimonio informativo del Dipartimento del Tesoro*** Giuseppe Maresca, Dirigente Generale
10:30	*Il piano di formazione e comunicazione SIMEC rivolto agli Enti esterni* Col. Mauro ODORISIO
10:40	*L'acquisizione dei dati e la fase di go-live del SIMEC. Analisi tecnica* Umberto Mascia (UCID)
11:00	Coffee break
11:30	*L'allargamento della base informativa:* *istituti di pagamento e prospettive di modifica normativa* Antonio Adinolfi
11:40	*La divulgazione dei dati: un rapporto mensile sulle frodi con carte di pagamento* Stefano Grossi (SOGEI)
11:50	*Nuove frontiere: la lotta al furto d'identità* Augusto Santori (Ufficio VI)
12:10	*La gestione della sicurezza nel sistema dei pagamenti* Monica Pellegrino (ABI Lab)
12:30	*Varie ed eventuali*
12:50	*Chiusura dei lavori* Antonio Adinolfi

"Il Gipaf torna a riunirsi, primariamente per rendicontare del lavoro svolto, che ha portato alla definitiva implementazione del SIMEC, il Sistema Informatizzato Monitoraggio Euro Carte. Un impegno preso dalla nostra Direzione qualche mese fa, frutto di un lungo lavoro, complesso, articolato e risultato di un'attiva, quasi costante, sinergia tra i nostri uffici, Ucid e Sogei, e realizzato naturalmente anche grazie al prezioso contributo di Abi e dei tanti stakeholders, che in questi mesi sono stati in ininterrotto contatto con la Direzione. Un ringraziamento particolare va proprio in questo senso anche a Banca Italia, all'IPZS e al Ced Interforze, per la loro disponibilità a far sì che questo strumento potesse diventare veramente un patrimonio di natura informativa al servizio di altri enti pubblici oltre che del settore privato", sono state le parole introduttive del Direttore Maresca, il quale ha annunciato il go-live del SIMEC per il 18 settembre .

Responsabile: Dott. Antonio Adinolfi
Dirigente Ufficio VI

Via XX Settembre, 97
00187 – Roma
Tel. 06 47610488
Web: http://www.dt.tesoro.it