La sicurezza delle informazioni nella società digitale

Ten. Col. Franco Sivilli
Ca. Uf. Informatica - Centro Nazionale Amministrativo
Comando Generale dell'Arma dei Carabinieri

Roma, 12 maggio 2017

Agenda

- Elementi di sicurezza
- Evoluzione tecnosociale della Rete
- Prospettive: Cloud & Big Data
- Riflessi criminologici
- Il lato oscuro della Rete

ELEMENTI DI SICUREZZA

Definizione di sicurezza

Lo stato o condizione nel quale le misure protettive adottate, garantiscono il mantenimento delle funzioni e prestazioni richieste ed il contenimento del DANNO entro limiti accettabili PRESTABILITI (rischio minimo), anche in presenza di minacce capaci di sfruttare le vulnerabilità del sistema.

"...sicurezza non vuol dire solo tecnologie, prodotti ed architetture ma anche comportamenti, soluzioni organizzative, procedure e soprattutto diffusione della cultura relativa..."

I principi di sicurezza

Confidenzialità (o riservatezza o segretezza): le informazioni devono essere accessibili solo a chi è autorizzato (soggetti o entità sw/hw).

Integrità (o autenticità): le informazioni non devono essere modificabili (la cancellazione è una forma di modifica) da chi non è espressamente autorizzato. L'integrità si riferisce ai dati, mentre l'autenticità si riferisce alle persone fisiche coinvolte nelle comunicazioni.

Disponibilità: le informazioni devono essere utilizzabili quando occorrono, pensando anche alle evoluzioni dell'ICT.

Identificazione e autenticazione: devono essere assicurate anche per i processi;

Non ripudio: impossibilità di negare una transazione effettuata

D.I.O. (Defensive Information Operation): Detecting & Reacting.

Incidente

Ogni tipo di attacco, intrusione, malware o perdita di dati

IL 75% DEGLI INCIDENTI SONO CAUSATI DALL'INTERNO

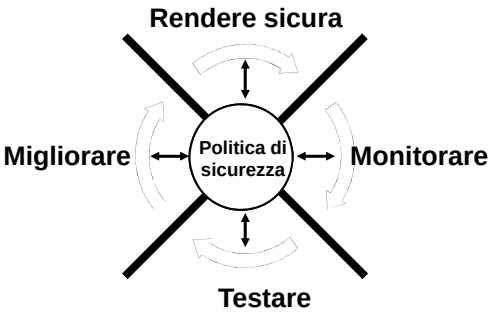
Sistema di sicurezza

Un sistema di sicurezza è l'insieme delle procedure e delle tecnologie adatte a proteggere ogni informazione da qualunque tipo di danno.

L'aumento del grado di sicurezza riduce la piena ed incontrollata libertà di accedere a qualunque dato

Metodologie di protezione

Cisco course CSIDS

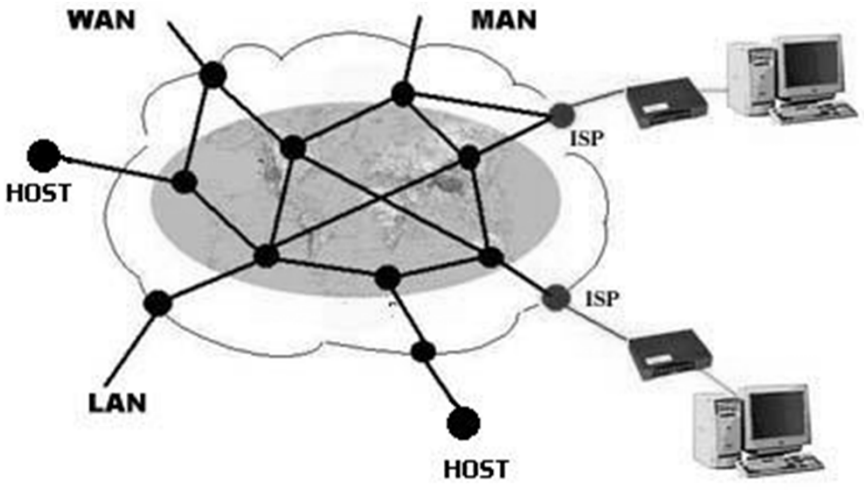


1. Comportamenti e procedure sicure (policy)
2. Protezione delle postazioni personali (Security Suite)
3. Protezione della rete (firewall, IDS, VPN)
4. Protezione delle informazioni (crittografia)
5. Misure di prevenzione perdita informazioni (sistemi fault tolerant, impianti elettrici, backup e Disaster Recovery)
6. Auditing e revisione continua dei punti precedenti

EVOLUZIONE TECNOSOCIALE DELLA RETE

Struttura della Rete

TCP/IP : In Italia 30 aprile 86

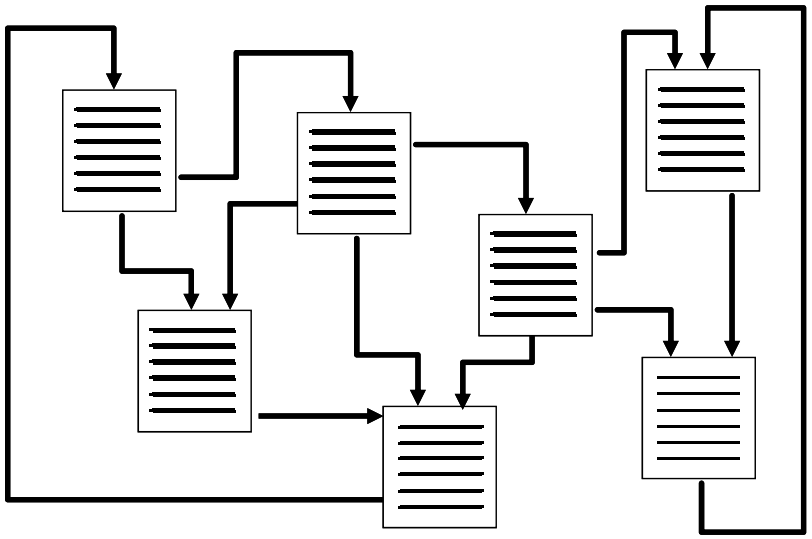


Ipertesto

HTTP

HTML

12 MAR 1989 : NASCITA DEL WEB



Web 1.0

E' la prima fase del Web, caratterizzata dalla progressiva definizione degli standard tecnologici che hanno permesso di dare vita a questa nuova realtà e di diffonderne l'uso tra milioni di utenti.

Affermatosi e diffusosi negli anni '90, il Web 1.0 è composto prevalentemente da siti web statici, senza alcuna possibilità di interazione con l'utente eccetto la normale **navigazione** tra le pagine, l'uso delle e-mail e l'uso dei motori di ricerca.

Web 2.0

E' la fase attuale, caratterizzata da una partecipazione attiva degli utenti alla costruzione dei contenuti, alla loro classificazione e distribuzione.

Il **Web 2.0** indica genericamente uno stato di evoluzione di Internet (e in particolare del World Wide Web), rispetto alla condizione precedente. Si tende ad indicare come Web 2.0 l'insieme di tutte quelle applicazioni online che permettono uno spiccato livello di interazione sito-utente (blog, forum, chat, sistemi quali Youtube, Facebook, Twitter ecc.).

Il Social Networking

E' il fenomeno che guida il Web 2.0.

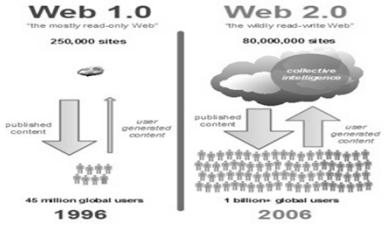
Si tratta di piattaforme di aggregazione sulle quali le persone possono entrare in contatto, condividere contenuti, stabilire nuovi legami o riproporre quelli della vita reale esaltando le caratteristiche principali del Web 2.0: la partecipazione e la condivisione.

Uso sicuro dei SN

1) Non pubblicare l'effettiva ubicazione quando si è in giro. Pubblicare ciò sui SN è una sorta di invito formale per i criminali.
2) Non pubblicare aspetti negativi della propria vita. Farlo è come screditare la propria immagine. I vostri Amici monitorano la vostra attività e uno sbaglio può causare danni in futuro.
3) Prendere distanza dal profilo dell'ex. Potrebbe sembrare crudele, ma una volta che si è deciso di uscire da una relazione non vi sono più motivazioni per visitare il profilo del proprio *ex-partner*. Se si vuole avere una vita tranquilla in futuro è consigliato cancellare il proprio ex dagli Amici.
4) Non sostituire gli amici reali con quelli virtuali. I SN sono un ottimo strumento per far interagire persone sparse per il mondo. Ma loro non saranno mai come i propri amici reali. Bisogna avere amici reali per accrescere se stessi e ridurre lo stress e l'ansia della vita reale.
5) Evitare di utilizzare i SN negli orari lavorativi. Utilizzare i SN durante il lavoro non influenza solo la propria *performance* ma aumenta anche la possibilità di essere licenziati.

Evoluzione della Rete

1. Anni '80 → La rete come mezzo per collegare computer
2. Anni '90→ La rete come strumento per collegare documenti (**Web 1.0**)
3. 3° Millennio:
   - la Rete come strumento di connessione delle relazioni sociali (Web 2.0)
   - Cloud computing → ICT: da strumento di gestione a strumento di governo
4. Scenari futuri : IoT e Web 3.0



… e all'orizzonte si intravede il Web 3.0….

PROSPETTIVE: CLOUD & BIG DATA

Cloud Computing

- Il "*cloud computing*" è un insieme di servizi (infrastrutture IT e applicazioni) offerti da appositi fornitori su Internet.
- Sfruttando la tecnologia del cloud computing gli utenti collegati ad un cloud provider possono svolgere tutte queste mansioni, anche tramite un semplice Internet browser.
- **Possono, ad esempio, utilizzare software remoti non direttamente installati sul proprio computer e salvare dati su memorie di massa on-line predisposte dal provider stesso (sfruttando sia Reti via cavo che senza fili).**

Cloud Computing

- Con il *cloud* diventerà sempre più sfumato il confine tra computer e Rete e sia l'infrastruttura che le applicazioni diventeranno un servizio
- (*Infrastructure as a Service+Software as a Service = Cloud*).
-
- Il computer del futuro, quindi, dovrà avere solo la potenza necessaria ad eseguire un browser come Internet Explorer (o *Firefox*, *Chrome*, *Safari*, e via discorrendo).

- Quando *Eric Schimdt* ha detto "*il browser è il computer*", si riferiva esattamente a questo.

Cloud Computing e sicurezza

Aspetti tecnologici

- Difficoltà a individuare la location geografica dei miei dati
- Chi tiene i miei dati e soprattutto quali vincoli o standard di sicurezza rispetta ovvero quali vulnerabilità del detentore dei miei dati potrebbero compromettere la loro integrità o quali perdite potrei subire se ci fossero dei disastri?
- Riusciamo davvero a disporre dei nostri dati e delle nostre applicazioni come se fossero in House?
- Quali rischi corriamo condividendo le nostre risorse con altri attori?

Cloud computing e sicurezza

Consigli del Garante per la Protezione dei Dati personali

- PONDERARE PRIORITARIAMENTE RISCHI E BENEFICI DEI SERVIZI OFFERTI;
- EFFETTUARE UNA VERIFICA IN ORDINE ALL'AFFIDABILITÀ DEL FORNITORE;
- PRIVILEGIARE I SERVIZI CHE FAVORISCONO LA PORTABILITÀ DEI DATI;
- ASSICURARSI LA DISPONIBILITÀ DEI DATI IN CASO DI NECESSITÀ;
- SELEZIONARE I DATI DA INSERIRE NELLA CLOUD;
- NON PERDERE DI VISTA I DATI;
- INFORMARSI SU DOVE RISIEDERANNO, CONCRETAMENTE, I DATI;
- ATTENZIONE ALLE CLAUSOLE CONTRATTUALI;
- VERIFICARE LE POLITICHE DI PERSISTENZA DEI DATI LEGATE ALLA LORO CONSERVAZIONE;
- ESIGERE E ADOTTARE OPPORTUNE CAUTELE PER TUTELARE LA CONFIDENZIALITÀ DEI DATI;
- FORMARE ADENGUATAMENTE IL PERSONALE

In prospettiva EU GDPR (mag 2018)

- **Data Protection Manager**
- **Profilazione**
- **Consenso nel web**
- **Dati genetici e sensibili**
- **Diritto oblio**

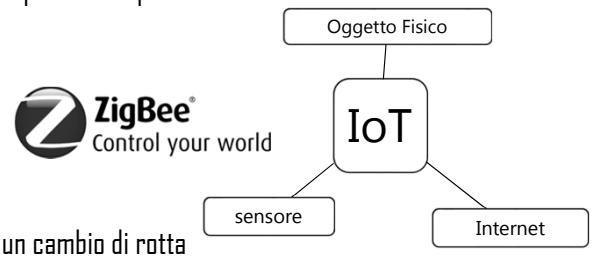
Cloud Computing e sicurezza

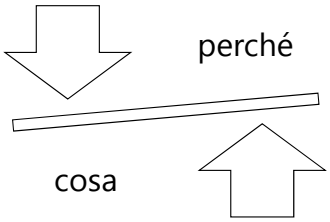
Criticità legali

- Cosa potrebbe verificarsi in caso di interruzione del contratto con il fornitore?
- E' possibile riportare il servizio presso la nostra sede fisica o dislocarle presso un altro fornitore?
- È possibile accertare la prova di un reato che prevede la detenzione di materiale informativo sul cloud ed acquisirne il contenuto utile ai fini forensi?
- Qual è il foro competente alla risoluzione di eventuali controversie legali?

IL DILUVIO DIGITALE

I Big Data rappresentano una raccolta estesa di dati su ampia scala resa disponibile dalla diffusione crescente dell'Internet of Things → dalla interconnessione delle persone a quella delle cose

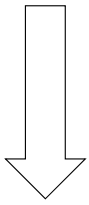




Si assiste ad un cambio di rotta
nell'analisi scientifica dei dati a disposizione,
dal principio di causalità al dominio delle probabilità

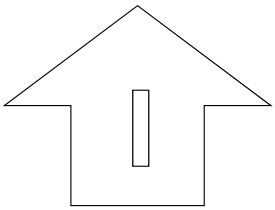
Digitalizzazione e Datizzazione

Digitalizzazione: consiste nel tradurre informazioni analogiche (suoni/immagini/documenti) in forma digitale (sequenze binarie).

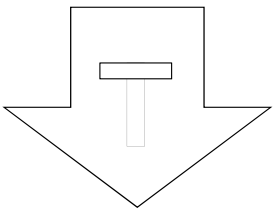


Datizzazione: significa convertire un fenomeno in forma quantitativa, così da poterlo tabulare e studiare.

Evoluzione dell' Information Technology



L'informazione diventa un bene immateriale, merce di scambio e risorsa di business



Ormai ampiamente diffusa in ogni settore, passa in secondo piano rispetto al ruolo centrale assunto dai dati

La rivoluzione dell'IT si è spinta finora sulla Technology, il futuro si spinge sull'Information

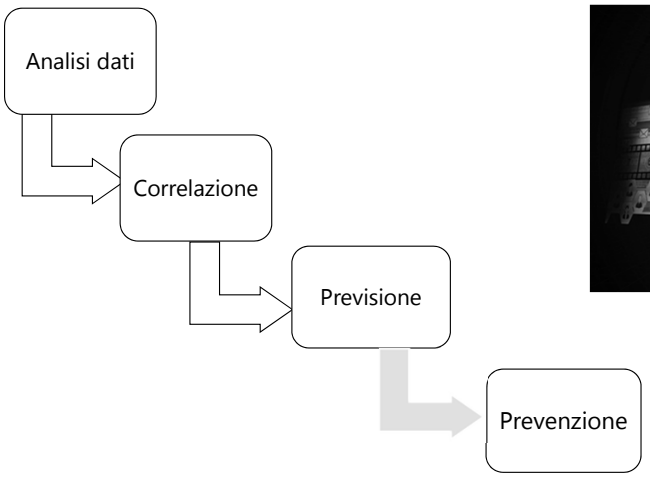
BIG DATA: la fine della teoria e l'inizio della datizzazione?

- Chris Anderson (Wired): Il **diluvio digitale** rende il processo tradizionale su cui si fonda la scoperta scientifica (un'ipotesi che viene testata rispetto alla realtà utilizzando un modello di casualità sottostante) destinato all'estinzione **per essere sostituito da un'analisi statistica di pure correlazioni del tutto svincolata dalla teoria** → Google usava le key-words e non i dati sanitari delle persone come indicatore rappresentativo dell'influenza.

BIG DATA

- Un team IBM e Univ. Ontario coordinati dalla dott.ssa McGregor sta sperimentando un sw che analizza 16 parametri diversi di neonati prematuri generando 1250 data point al secondo prevedendo, attraverso la loro correlazione, una infezione 24 ore prima della comparsa di sintomi evidenti. E' stato scoperto (contro la logica medica) che la stabilizzazione dei prematuri precede spesso una infezione grave. I dati suggeriscono una correlazione e non un rapporto di causalità. Per fare emergere questa associazione si sono dovuti applicare metodi statistici a un'enorme quantità di dati
- *L'allarme precoce permette un trattamento più tempestivo→ i big data potranno salvare delle vite!!!*

L' obiettivo dei Big data



Lo scenario futuro: evoluzione nel Web semantico

"il Web Semantico è un'estensione del Web corrente in cui le informazioni hanno un ben preciso significato e in cui computer e utenti lavorano in cooperazione".

Trasformare il Web in un database

Monitoraggio h24?

RIFLESSI CRIMINOLOGICI

Riflessi criminologici

L'influenza delle nuove tecnologie informatiche agisce sulla criminalità tradizionale modificando le forme classiche di reato, in nuove forme di reato, alterando pertanto i processi di percezione del crimine.

Impatto psicologico

I comportamenti illegali detti "tecnomediati" possono essere effettuati anche da soggetti che difficilmente eseguirebbero analoghe azioni in ambito reale o non digitale

L'impatto "face-to-face"non è poi cosi facile da sostenere

Impatto psicologico

Internet ha ampliato il potenziale delle possibili vittime e ha anche reso il lavoro delle forze dell'ordine sempre più difficile.

A differenza di un crimine tradizionale, in cui vi sono testimoni oculari, nessuno può vedere un crimine che ha luogo su Internet.

Alcuni pericoli della Rete

La dipendenza dai new Media (videogiochi, gioco d'azzardo etc)
Violazione copyright, furti o distruzione di informazioni
Frodi informatiche
Negazione servizi web
I furti di identità e di denaro nella Rete
Il cyberstalking, cyberbullismo, child grooming e cyberpedofilia, cyberterrorismo

Comitato nazionale per la ricerca in cyber security (CNR e CINI) feb 2017

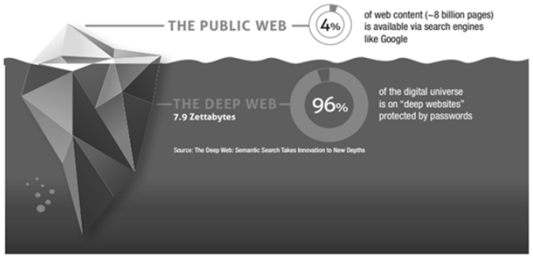
Progettare un ecosistema nazionale più resiliente agli attacchi cyber;
Migliorare la continuità di servizio delle infrastrutture critiche, della pubblica amministrazione e delle filiere produttive strategiche;
Sviluppare piani di formazione per aumentare la 'workforce nazionale' in cybersecurity;
Migliorare la consapevolezza di imprese e cittadini rispetto alle minacce cyber;
Infittire la collaborazione con organizzazioni omologhe europee e internazionali

400 Miliardi di dollari all'anno, pari all'0,8% del PIL mondiale, il costo globale del cybercrime (McAfee)

IL LATO OSCURO DELLA RETE

Origini e dimensioni del DEEPWEB

Il termine **"deepweb"** è usato per indicare una classe di contenuti su Internet che, per diversi motivi tecnici, **non è indicizzato dai motori di ricerca (500 volte il web visibile).**



Nasce per:

comunicare in maniera anonima in Rete;

salvaguardare il *diritto alla privacy* degli utenti;

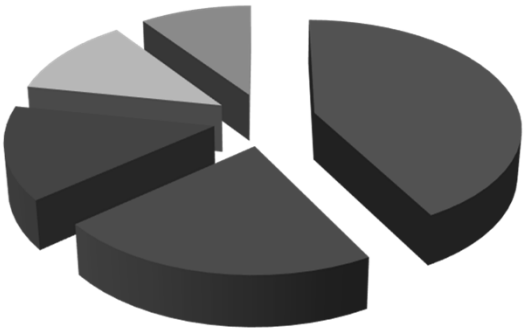
MA

La libertà di pensiero ed espressione in un territorio virtualmente infinito comprende anche gli

ABUSI DI CHI APPROFITTA DI QUELLO SPAZIO PER DELINQUERE.

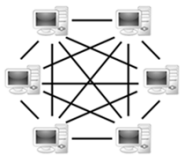
Gli utenti

- Attivisti informatici, politici e religiosi (informazioni sensibili es. wikileaks)
- Servizi di prevenzione per sondare pericoli internazionali e per catturare tendenze in anteprima;
- Professionisti delle informazioni (*data mining* o *information brokering)*
- Dark user: utenti della darknet (la parte illegale della Rete)



Il Deep Web: le reti che lo compongono

TOR* P2P FREENET



* La più usata

Il Deep Web: la rete TOR

La rete TOR è stata originariamente sviluppata dalla US Naval Research Laboratory ed introdotta nel 2002 per consentire comunicazioni anonime tramite una rete basata su una serie di nodi chiamati relay, costituiti da server intermediari (onion) attraverso i quali transitano i dati prima di arrivare a destinazione.

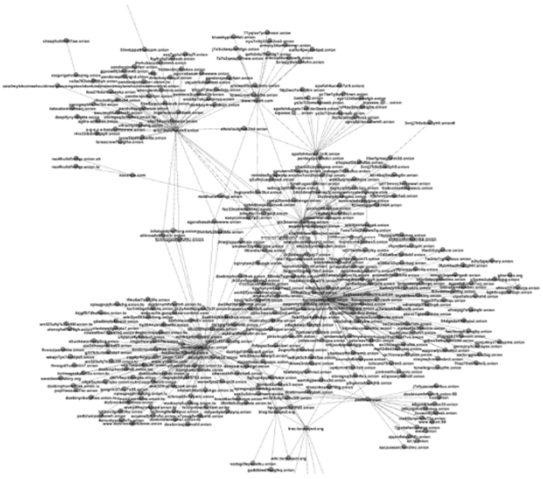
In pratica, i dati prima di arrivare al server del sito web richiesto, passano in questi nodi casualmente utilizzando sempre un percorso differente. Arrivati al nodo prescelto, viene selezionato immediatamente il successivo e così via. La rete è strutturata in modo tale da modificare il percorso dei dati ogni dieci minuti e automaticamente. Ne consegue che i siti web non capiscono da dove ricevono la richiesta. Per aumentare la sicurezza, tutti i dati scambiati tra i server sono crittografati in modo tale da impedirne la lettura.

Il Deep Web: la rete TOR

- **Si accede con un client TOR**

- **Si naviga attraverso:**
  - ✓ **la hidden Wiki (una lista di siti .onion linkati ed accessibili suddivisi per categoria);**
  - ✓ **un motore di ricerca ad hoc denominato *torch search engine*;**

Il Deep Web: la rete TOR (meno connessioni) (i nodi onion censiti)



Il Deep Web: i contenuti

- Portali pedopornografici come Lolita City o OnionPedo;
- Portali per rovinare in maniera anonima la reputazione di terzi come RespiraTor;
- Laboratori rivoluzionari politico-informatico come Revolution Bunker o LiberaTor per costruirsi un arsenale domestico, confezionare ordigni esplosivi e organizzare agguati e attentati
- Hacker Services che mette a disposizione virus informatici per attaccare persone o aziende sgradite e sistemi di ricerca delle password altrui;
- Contract killer: offre omicidi a pagamento, con tariffe dettagliate. Cinquemila euro di spese anticipate per un delitto in Europa, diecimila per una trasferta extracontinentale. C'è una sorta di regolamento: l'obiettivo deve avere almeno 16 anni, e il costo dell'operazione è di 20 mila euro per una persona normale, 50 mila per un poliziotto, un criminale o un paparazzo, 100 mila per un boss, un funzionario di polizia o un giornalista, fino a 200 mila per un manager. Due mesi di tempo dal primo pagamento per completare la missione.

… qualche numero

La crescita è circa il 30% più veloce della Rete normalmente accessibile a causa del timore della censura

Ogni giorno circa 200.000 $ di transazioni finanziarie quasi esclusivamente droghe

Il 20% degli oltre 500 milioni di doc sono correlati alla pedofilia

Il Deep Web: la moneta

Gli acquirenti e i venditori di questi siti, conducono tutte le loro transazioni con il **Bitcoin**, una moneta virtuale detta anche criptomoneta, che si basa sul concetto dell'anonimato e della prova di scambio, oltre ad avere, di norma, uno schema di emissione pre concordato. Valute di questo tipo hanno poco a che fare con quelle emesse dalle banche nazionali. La loro nascita risale idealmente alla fine del 2008 da Satoshi Nakamoto che pubblicò sul sito *metzdowd.com* un documento chiamato Bitcoin sancendo la nascita dell'idea alla base di tutte le criptomonete.

1 Bit Coin vale circa 400 €

Il Deep Web: non è tutto negativo

Ian Walden (professore di Information and Communications Law alla *Queen Mary University* di Londra) sottolinea che « nei regimi dove la censura è all'ordine del giorno, i social media non favoriscono le proteste politiche, poiché è molto facile identificare gli utenti» e che il deepweb permette di «comunicare nel lungo periodo senza mettere a rischio l'incolumità dei propri cari».

TOR per i giornalisti è una vera manna, serve per poter comunicare segretamente con le loro fonti.

fsivilli@carabinieri.it