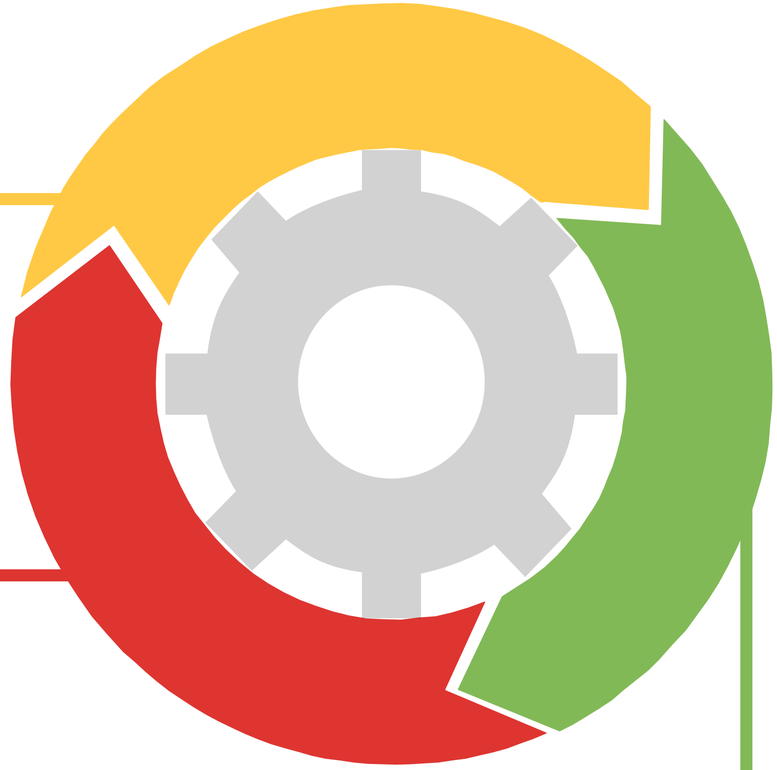
Giuseppe Augiero

I PERICOLI DEL DEEP WEB E IL SISTEMA INFORMATIVO SANITARIO

18 dicembre 2015 - Privacy e sicurezza in sanità: strategie manageriale profili di responsabilità - Auditorium Palazzo dei Congressi di Pisa

EQUILIBRIO PERFETTO

1. INFORMAZIONE
2. SECURITY
3. PRIVACY



SECURITY

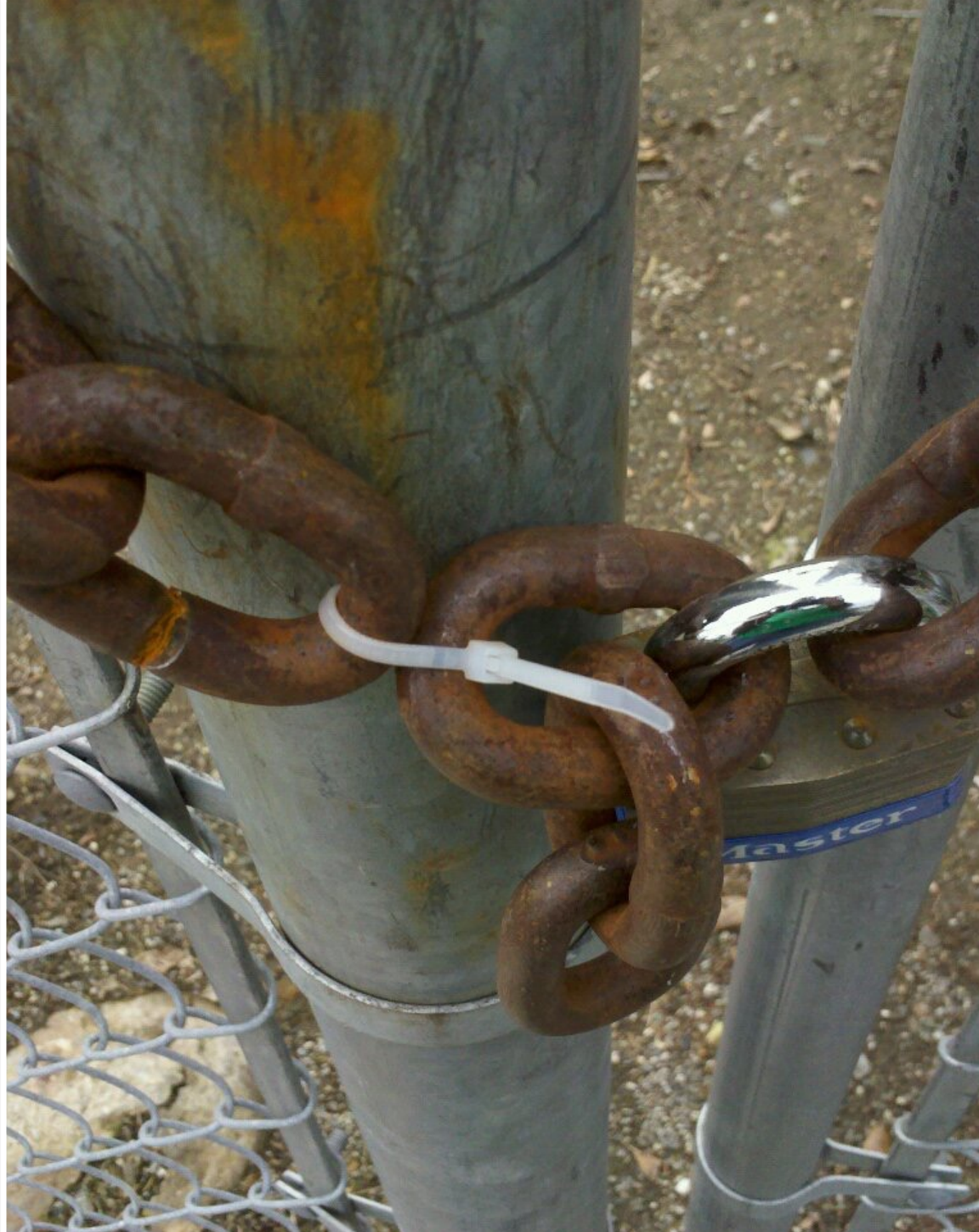
I PRINCIPI DI BASE

- Occorre garantire:
  - la correttezza dei dati (integrità).
  - la confidenzialità dei dati (cifratura);
  - l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
  - la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
  - la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti.

SECURITY

LA CATENA DELLA SICUREZZA

- Per misurare il grado di robustezza di un sistema occorre valutare la componente che rappresenta l'anello più debole della struttura.
- Trade-off (usabilità).
- Molto spesso si reputa che l'anello più debole sia rappresentato dall'utente.



NON SEMPRE OCCORRE UN ATTACCO

(ALCUNI CASI RECENTI)

UTENTE SVOGLIATO

MISCONFIGURATION - ISP

28 VOLTE - PROGRAMMATORI


Firewall
security
network
connection
filters
rules
application
layer
filter
block
internal
packets
server
protected
term
internet
private
traffic
admin
edit
firewalls
www
UDP
hardware
transfer
generation
control
IP
protocol
zone
information
configuration
developing
trust
destination
packet
intranet
hosts
TCP
translation
software
prevent
ports
technology
computer

L'INFORMAZIONE

CICLO DI VITA

- Alcune informazioni di identificazione personale possono avere un ciclo di vita più lungo rispetto ad altre informazioni.

- Maggiore è il ciclo di vita e maggiore è il loro valore dal punto di vista economico.

    - Un dato bancario ha una durata, nel caso di una carta di credito, di max 5 anni.
    - Un dato sanitario, invece, dura tutta la vita.

L'INFORMAZIONE

ATTORI E COSTI

- Chi acquista i dati sanitari?
  - Imprese assicuratrici.
  - Imprese del settore medico.
  - Casa farmaceutiche.

- Borsino dei dati:
  - Mille carte di credito: **70$**
  - Account Paypal: **250$**
  - Credenziali Bancarie: **500$**
  - Dato Sanitario: **1000$**

L'INFORMAZIONE

ALCUNI CASI

- Ashley Madison
- Hacking Team
- Target
- Apple (user)

L'INFORMAZIONE

WHERE?

- Dove vanno a finire i dati sottratti sul web?
- Dove è possibile acquistare i dati?

- In ogni caso parliamo di attività illecite.

- *Buona parte dei dati sottratti attraverso attività illecite finiscono nel* ***Deep Web****.*

DEEP WEB

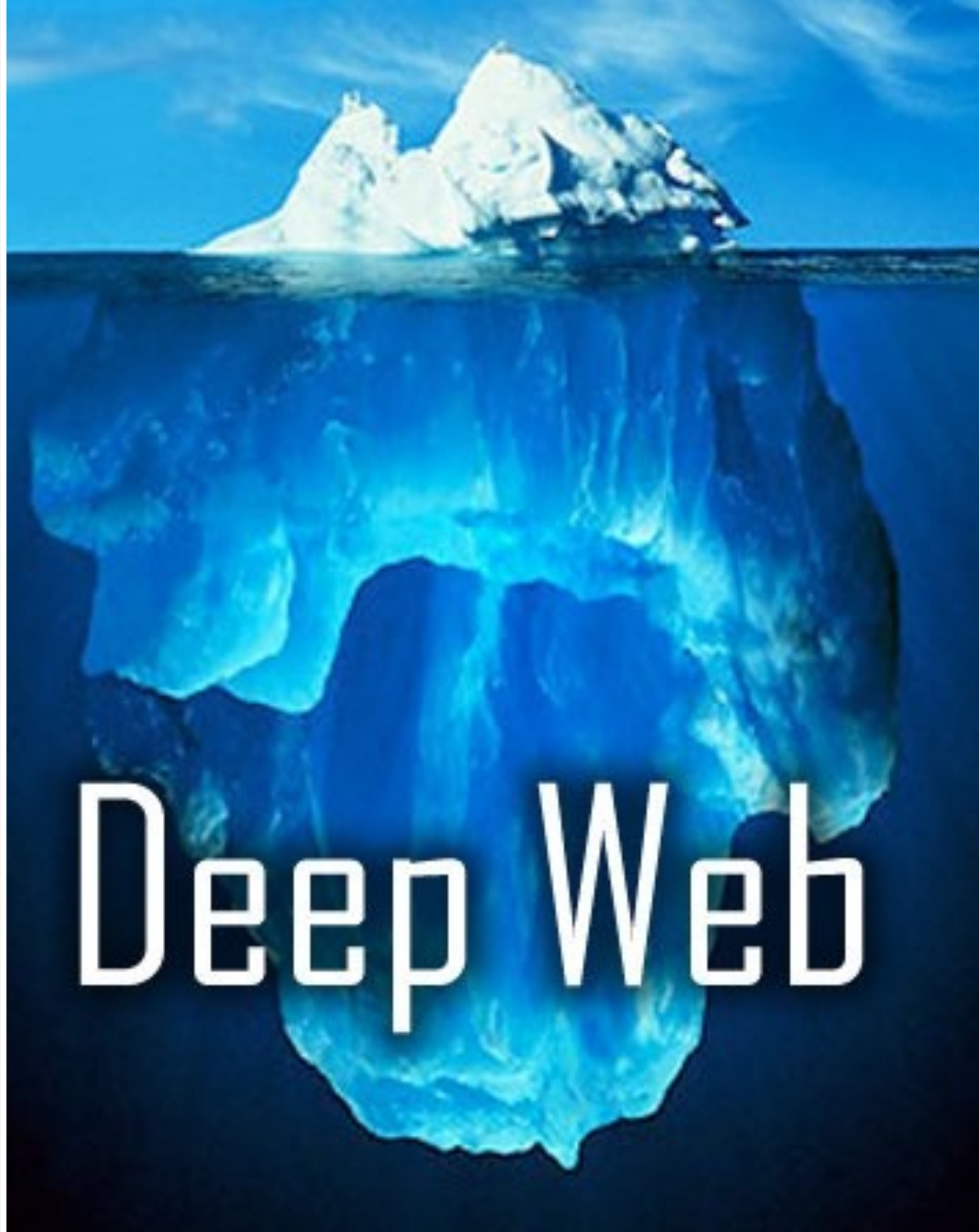
DEEP WEB

“Esiste una Internet, invisibile e nascosta, poco conosciuta dai più ma molto più densa...”

DEEP WEB

WHAT?

- Il Deep Web è la parte nascosta del Web.
- Inaccessibile dai tradizionali motori di ricerca e, di conseguenza, dalla maggior parte degli utenti.
- Le pagine sono generate dinamicamente in base alle richieste degli utenti. Non esistono pagine statiche o persistenti.
- “Hidden Databases” e Leak.



DEEP WEB

QUANTO È GRANDE?

- Il Deep Web ha dimensioni decisamente più grandi rispetto al web.
- Il rapporto tra deep e web è di almeno ***500 volte*** (7500 Tb vs 19 Tb).
- Non sono conosciuti gli esatti confini del Deep Web.
- Dove risiedono i contenuti?

DEEP WEB

SEARCH ENGINE

- I motori di ricerca che quotidianamente usiamo non riescono a catalogare e indicizzare le informazioni presenti nel Deep Web.

- Non esistono "***Web Directiories***" (Lycos, LookSmart) in merito.

- Un motore di ricerca come Google riesce a indicizzare solo il 5% di ciò che è online.

- Separazione Logica.

DEEP WEB

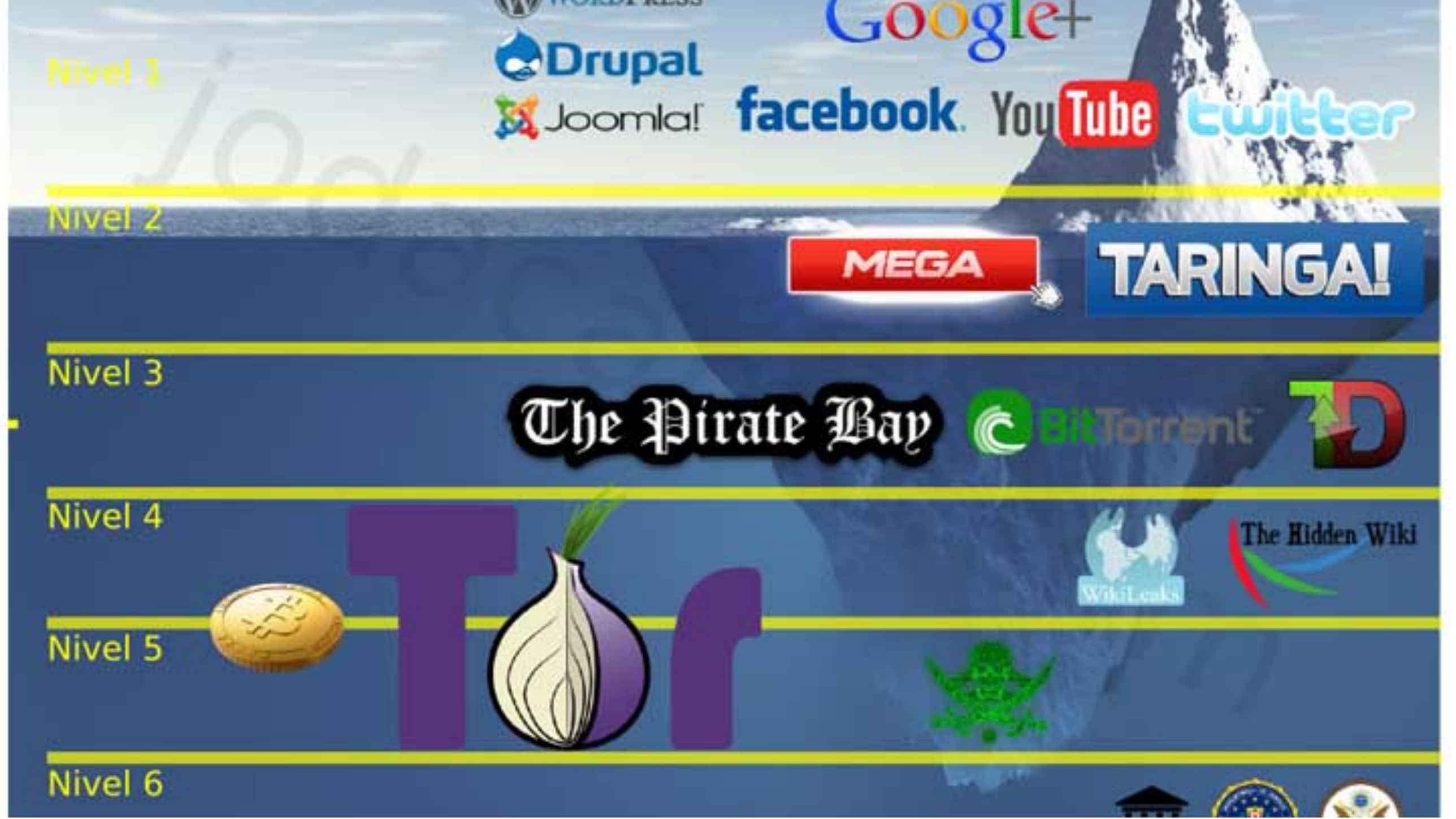
DATACENTER

- Il Dove si trovano i dati presenti nel Deep Web?
- Non esiste un datacenter o un luogo ben preciso dove risiedono.
- I dati sono distribuiti a livello mondiali e possono risiedere nello stesso server con il quale viene erogato un servizio Web.

DEEP WEB

COME ACCEDERE

- I normali browser non possono accedere alla “parte invisibile” di Internet.
- Gli indirizzi usati nel Deep Web non sono validi per l’uso comune.
- Esistono diversi modi per accedere ai “livelli” del Deep Web.
- Dal quarto livello occorre utilizzare ***TOR***.


Nivel 1
Drupal
Joomla!
Google+
facebook
YouTube
twitter
Nivel 2
MEGA
TARINGA!
Nivel 3
The Pirate Bay
BitTorrent
Nivel 4
Tor
WikiLeaks
The Hidden Wiki
Nivel 5
Nivel 6

DEEP WEB

CONTENUTI

- Database consultabili.
- E’ possibile scaricare file e fogli elettronici.
- Immagini e file multimediali.
- Pdf.
- Forum.
- Informazioni governative.

- **Alcuni dati sono provenienti da data-breach o leak**.

DEEP WEB

MOTIVAZIONI

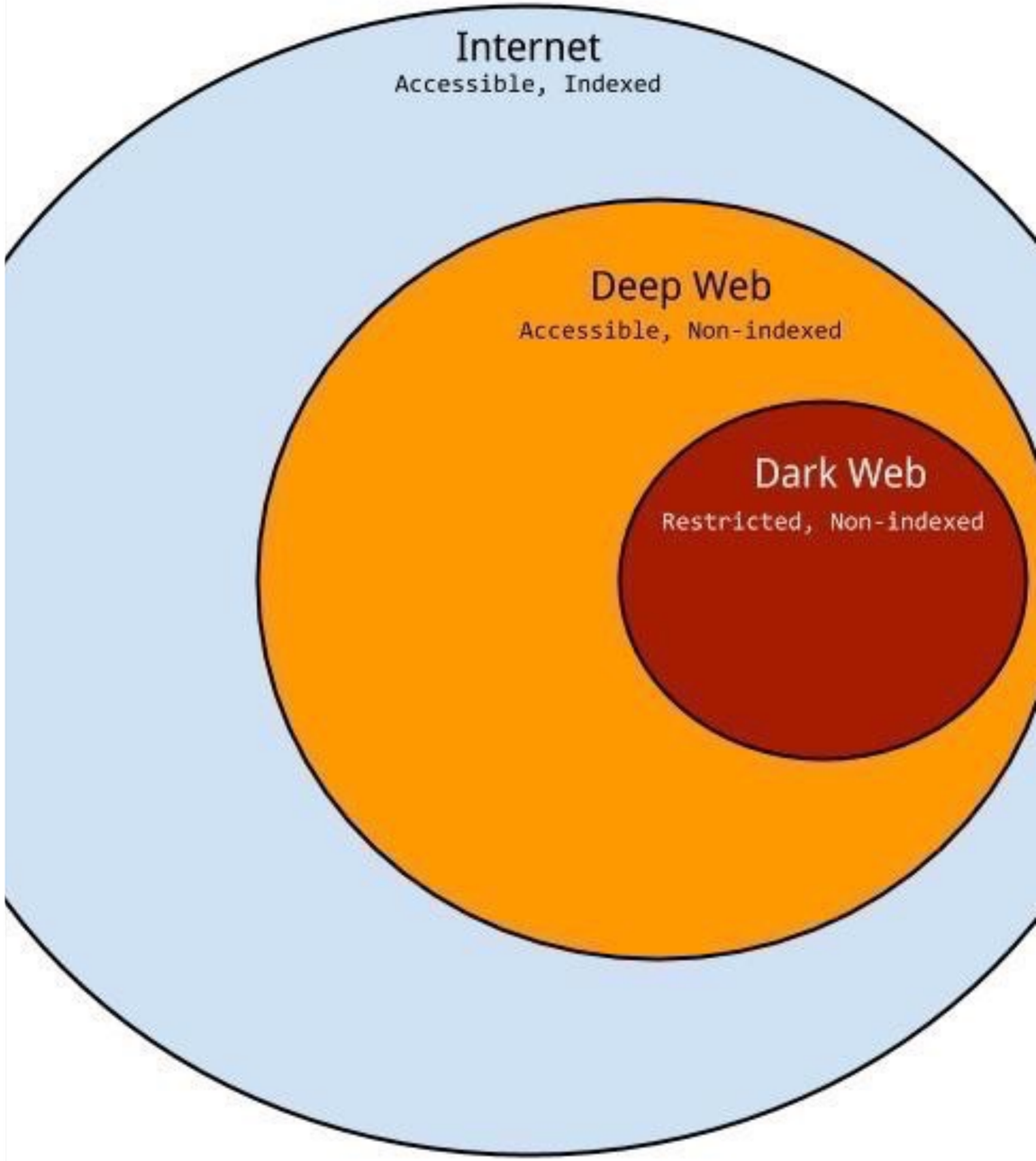
- Le principali motivazioni per frequentare il Deep Web sono:
    - Privacy.
    - Anonimato.
    - Impossibilità del tracciamento della connessione.
    - **Accesso a informazioni riservate.**
    - Nessuna censura.

DARK WEB

DEEP WEB VS DARK WEB

- Esiste un sottoinsieme del Deep Web, il cui accesso è molto ristretto e il contenuto non è indicizzato che prende il nome di Dark Web.

- Siti e servizi.



DARK WEB

SOLDI, SOLDI, SOLDI!

- Arrivano, dal dark web, nuove minacce per le aziende sanitarie.
  - **Ramsonware.**
  - **Rat.**
- Il pagamento avviene attraverso la criptovaluta Bitcoin.

DARK WEB

CRIMINALI

- A coloro che sono interessati realmente alle “informazioni sottratte illecitamente”, si vanno a sommare i criminali che vedono nella rivendita dei dati o nell’estorsione per il decrypt di essi, la benzina per il sostentamento delle loro attività.

IN CONCLUSIONE

COSA FARE?

COOPERAZIONE

SISTEMI ESPERTI

FORMAZIONE

CONSAPEVOLEZZA

- LO SCOPO ULTIMO DEVE ESSERE QUELLO DELLA PROTEZIONE DEI DATI DEI PAZIENTI.

THANK YOU

GRAZIE PER L'ATTENZIONE

EMAIL: GIUSEPPE@AUGIERO.IT

TWITTER: @GIUSEPPEAUGIERO

WWW.AUGIERO.IT

Giuseppe Augiero

I PERICOLI DEL DEEP WEB E IL SISTEMA INFORMATIVO SANITARIO

18 dicembre 2015 - Privacy e sicurezza in sanità: strategie manageriale profili di responsabilità - Auditorium Palazzo dei Congressi di Pisa