

Il ruolo della Cyber Security nello scenario dei social media

Fabrizio De Santis – 09/06/2016

BUSINESS-E SPA

SPECIALISTI IN CYBER SECURITY

RAVENNA (HQ) | MILANO | ROMA | MASSA | TRENTO | NAPOLI | BARI | VICENZA



FATTURATO

120 milioni



PROFESSIONISTI

Oltre 300



CERTIFICAZIONI

Oltre 700



SEDI

18

GRUPPO ITWAY

LE SEDI

RAVENNA (HQ) | MILANO | ROMA | MASSA | TRENTO | NAPOLI | BARI | VICENZA



PARIS | MADRID | BARCELONA | LISBOA | ATHINA | ISTANBUL | ANKARA | DUBAI | TEHERAN



FATTURATO

120 milioni



PROFESSIONISTI

Oltre 300



CERTIFICAZIONI

Oltre 700



SEDI

18

SERVIZI

SICUREZZA INFORMATICA E INFRASTRUTTURA IT



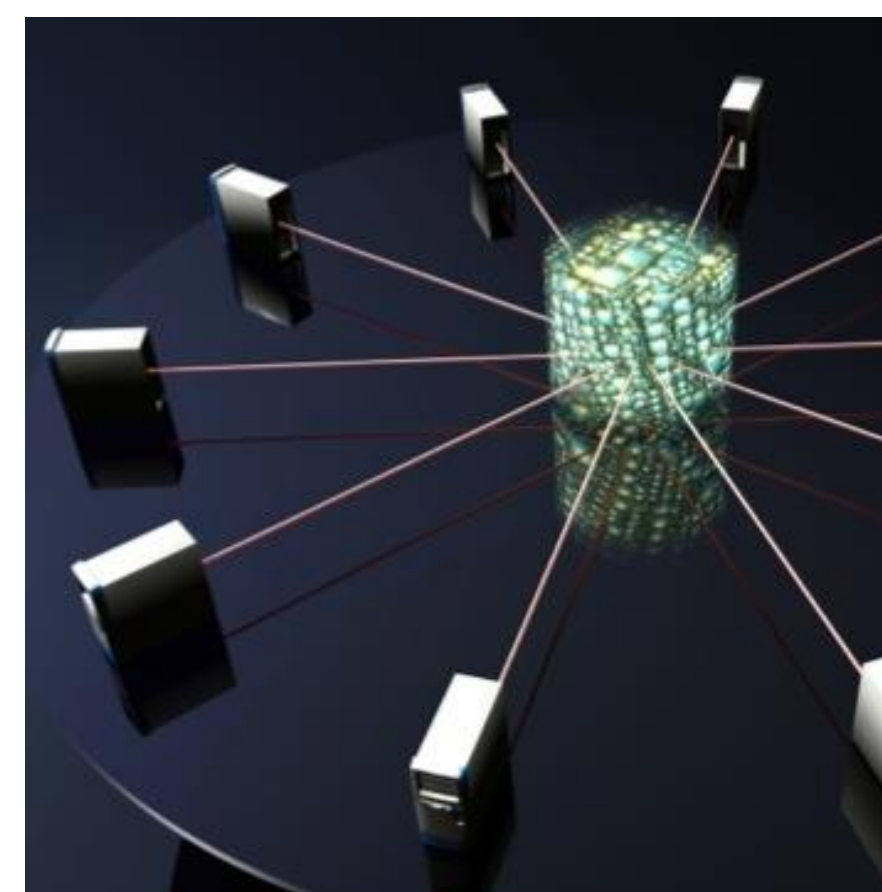
Security Consulting

Gestione della sicurezza:
dalla prevenzione alla difesa



Sicurezza Informatica

Grazie a partnership
strategiche con i migliori
Vendor sul panorama
mondiale, forniamo servizi di
sicurezza informatica



Infrastruttura IT

Ottimizzazione dei Datacenter
e servizi sulle infrastrutture di
rete con forte specializzazione
sulle soluzioni Open Source



Cyber Security Services

Outsourcing dei servizi
di Cyber Security per
aumentare la redditività,
ottimizzare i costi di esercizio e
migliorare la sicurezza dei dati
e dei processi

Il web 2.0

Il concetto di «Web 2.0» ha fatto la sua prima comparsa nel 2004 (*):

- come strumento collaborativo;
- con lo scopo di raccogliere i singoli contributi di milioni di persone e valorizzarli.

La transizione da 1.0 a 2.0 ha implicato un upgrade sia tecnologico che concettuale. Compagnono nuove tecnologie in grado di:

- consentire l'interazione:
 1. tra utenti in tempo reale;
 2. ad utenti anche inesperti;
- Offrire servizi complessi

Il web 2.0

Tecnologie

Client side

AJAX, Javascript, jQuery
DOM, JSON, XML, J2EE
YUI Library, Dojo Toolkit
syndication (Atom, RSS)
CMS

Concetti

E-commerce, Blog, wiki, social networks, social media
Hosted services
Cloud
Crowdsourcing, Crowdfunding
Tagging, «like»
Cost per click
Web Services
widget
PAAS, IAAS, SAAS
Spamming, trolling
Viral content

Servizi

Youtube, Vimeo, Netflix
Ebay, Amazon,
Facebook, Twitter, LinkedIn
Skype
Google Docs
Dropbox, Google Drive, One Drive
Wikipedia
Blogger, Wordpress, Reddit
Flickr
Last.fm, Spotify, Ad-Sense, etc..0

Il concetto di sharing

Anche gli utenti diventano «2.0»:

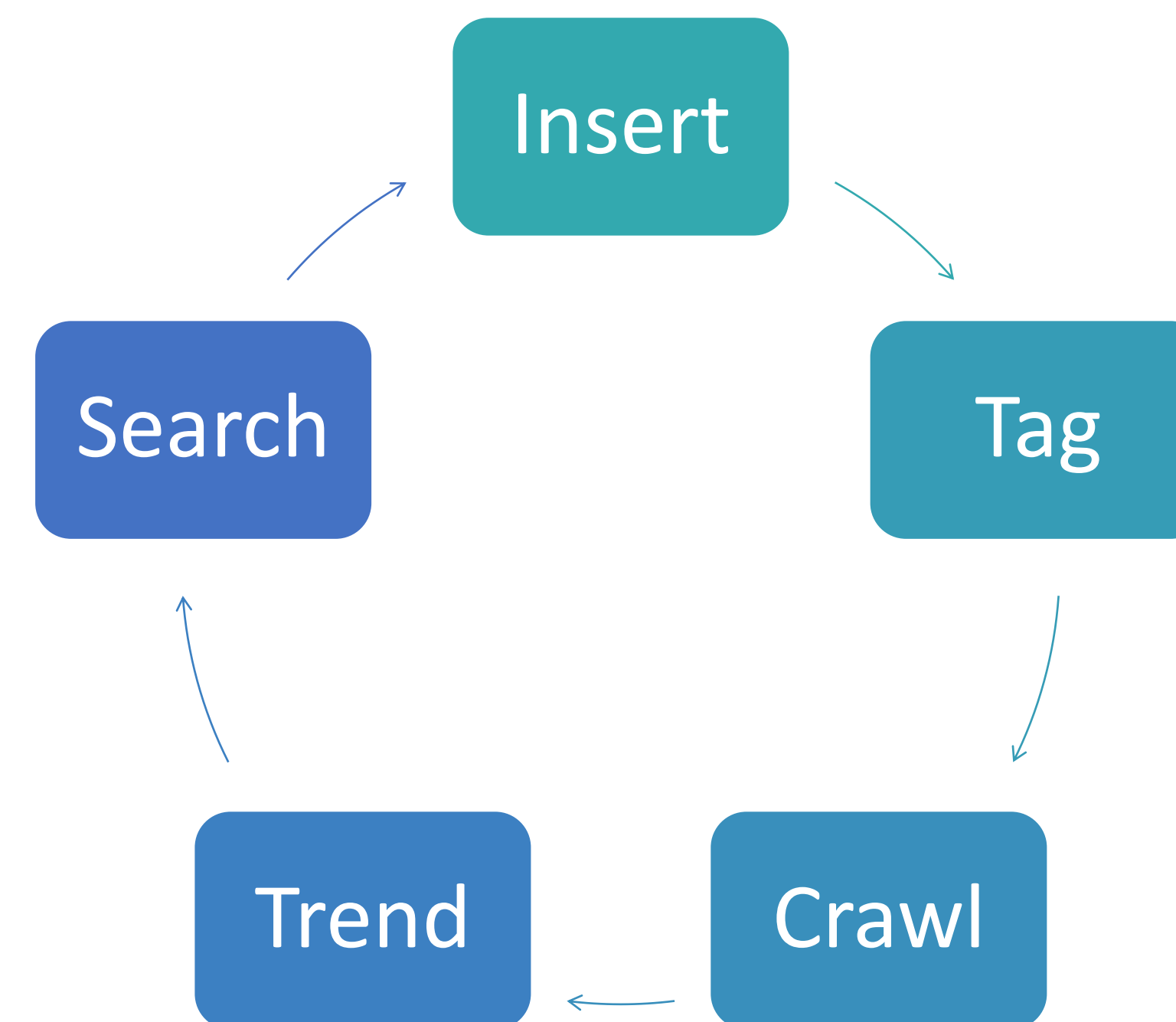
- interazione con i contenuti pubblicati attraverso commenti, retweet, feedback, tag, ... ;
- creazione account sul sito web;
- spamming, trolling, ... ;

Nasce il concetto di sharing.

Gli utenti condividono **file, conoscenza, idee**;

I contenuti sono:

- inseriti dinamicamente sui siti;
- organizzati logicamente (taggati);
- indicizzati dai crawler dei motori di ricerca;
- aggregati (RSS, trending, ...);
- ricercati da altri utenti.



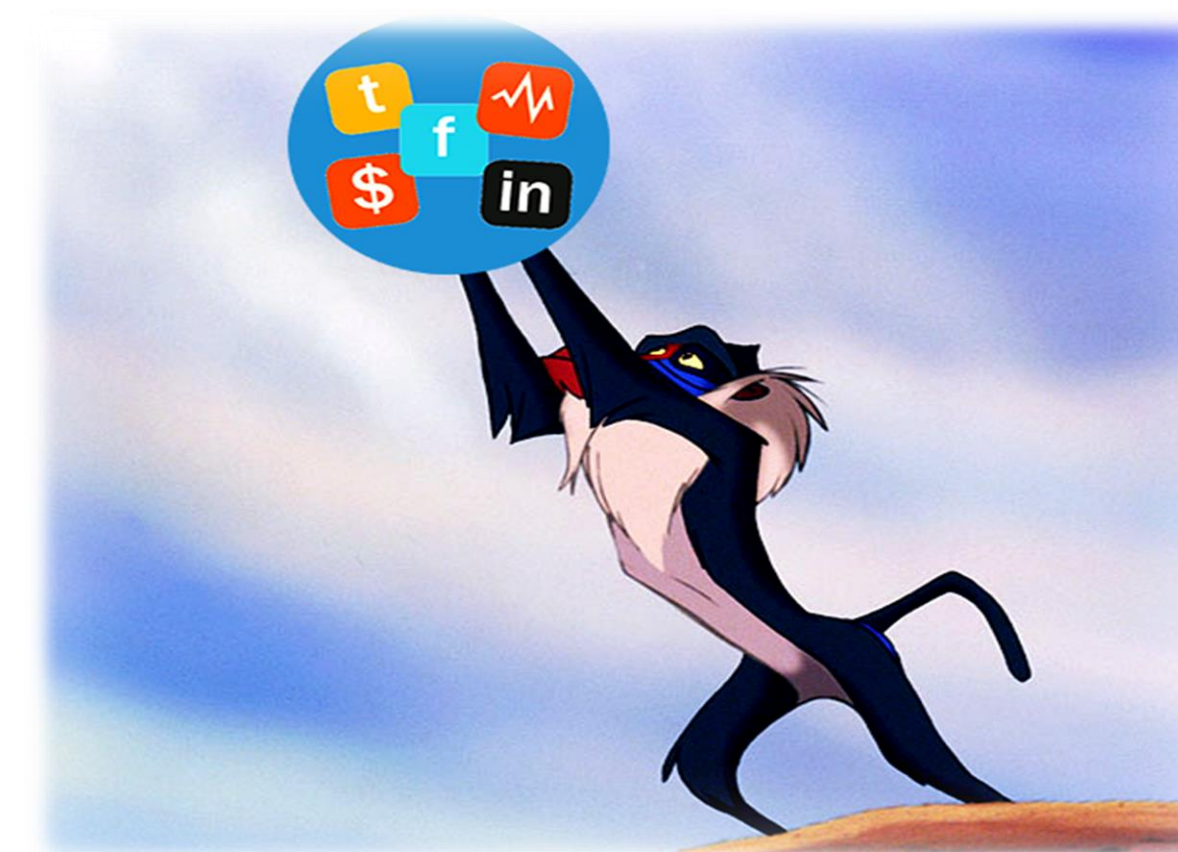
7 La potenza dei social media

Nascono i **social media** → **web come mezzo d'informazione**

I social media «rappresentano un cambiamento nel modo in cui la gente apprende, legge, condivide informazioni e contenuti».

Grazie alla fusione tra **sociologia e tecnologia**, l'informazione viene «democratizzata»;

- le persone si trasformano da fruitori ad editori;
- l'**audience** è globale (tutto il mondo);
- è un mezzo di informazione a **basso costo**;
- è accessibile a chiunque;
- le informazioni sono **disponibili** immediatamente;
- i contenuti vengono **replicati** ovunque;



Questi fattori rendono i social media strumenti estremamente **potenti...**
...ed **appetibili**

7 La pericolosità dei social media

Web 2.0 → Social Media → web come mezzo d'informazione

- Audience globale
- Rapidità di diffusione dell'informazione
- Accessibile a chiunque

I social media possono essere usati per arrecare danno.

- Disinformazione
- Information Leakage
- Terrorismo



L'entità del danno è proporzionale ai benefici che offre lo strumento di comunicazione

Cybercrime

Alcuni dati



Danni

Registrati nel corso del 2015 secondo il CLUSIT



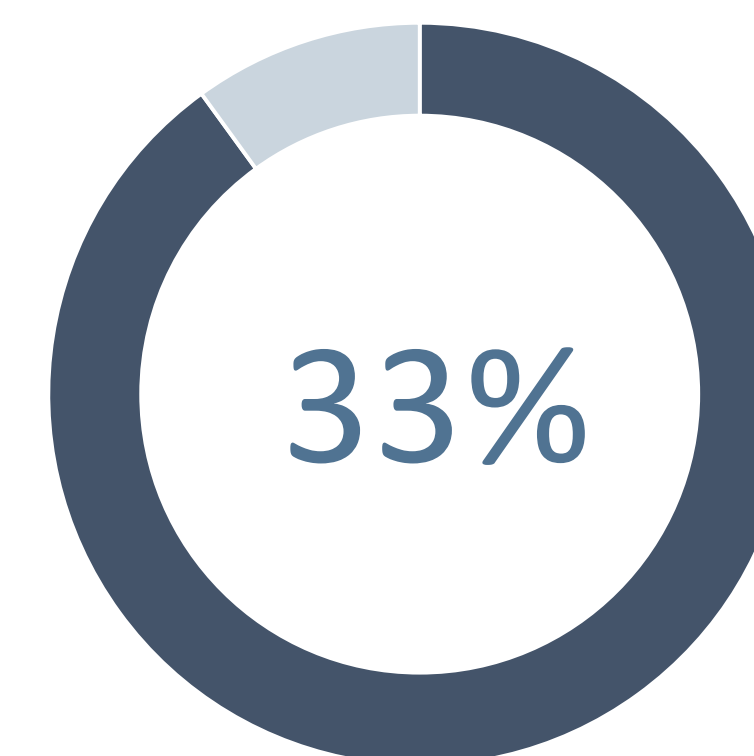
Cybercrime

Aumento del cyber Crime secondo il Rapporto Clusit 2015 (resoconto sulla sicurezza informatica)



Credenziali Rubate

Secondo il rapporto realizzato da Hold Security



Top Management

Considera la sicurezza informatica come una priorità d'investimento per la propria azienda

7 Gli Attaccanti

Ad opera di chi vengono fatti gli attacchi?

1

CYBER CRIMINALI

Social Media - Botnet - Targeted attack - Insider - Malware-as-a-service
- Deep Web

GOVERNI

Cyber Espionage - Digital War

2

3

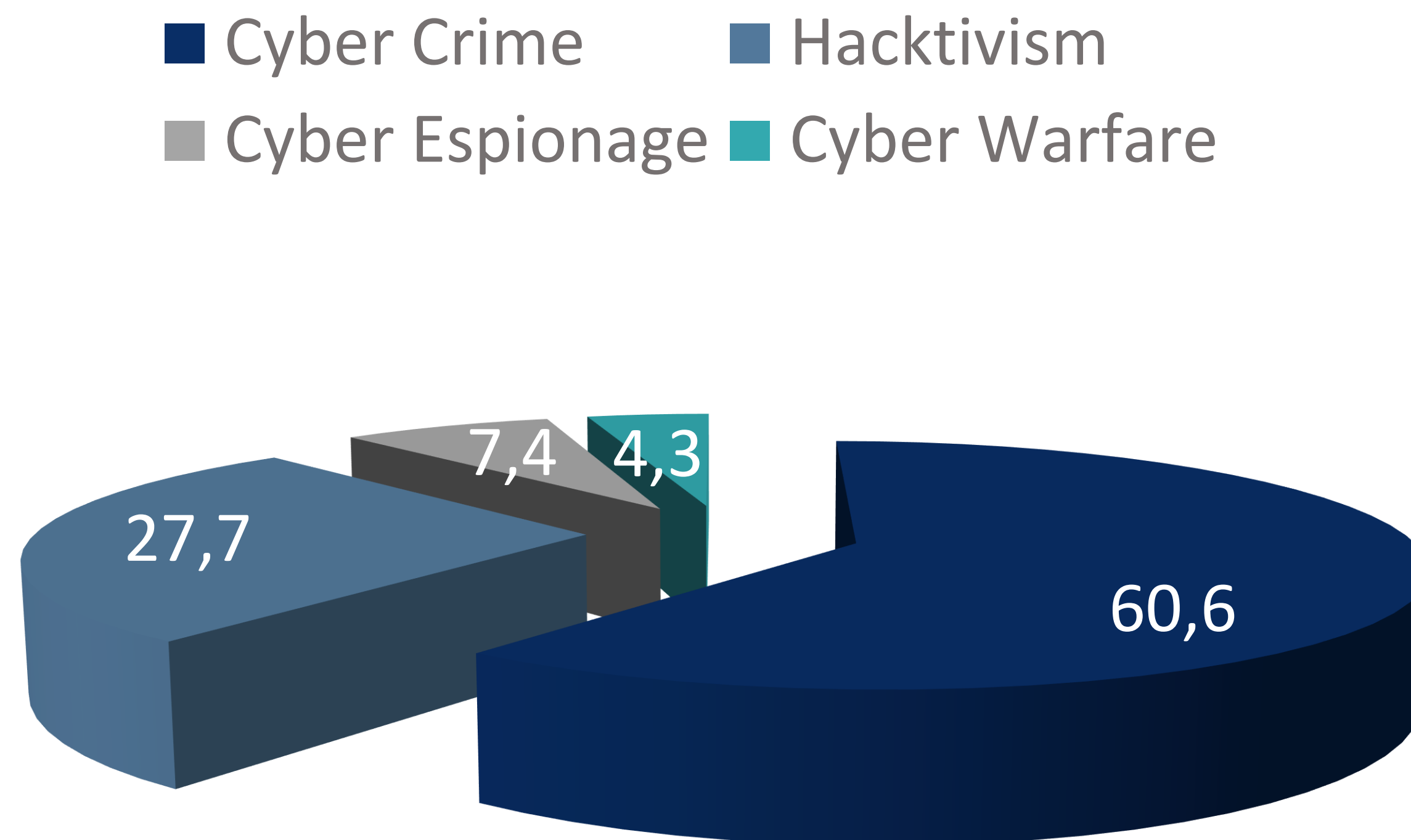
AZIENDE "LEGITTIME"

Che vendono veri e propri rootkit per la lotta al terrorismo, il supporto alle investigazioni, ma acquistati spesso in assenza di controlli sul loro effettivo utilizzo



Le motivazioni

- Guadagno personale
- Sfida/divertimento
- Estorsione
- Cyber War



<http://www.hackmageddon.com/2016/02/16/january-2016-cyber-attacks-statistics/>

Il rovescio del rovescio della medaglia

Come prevenire/arginare il danno derivante da un uso «doloso» dei social media?

la soluzione non è oscurare i contenuti

E' necessario puntare su una efficace Cyber Intelligence per fare **prevenzione e mitigare le minacce;**

Il Web 3.0 fornisce gli strumenti di base per fare Intelligence: nasce la figura del Big Data Scientist;

Unito a team di Intelligence...e alla ricerca di tecniche di analisi sempre più all'avanguardia

E' possibile sfruttare le informazioni raccolte dai social media per:

- tracciare, localizzare, prevenire le minacce
- tracciare pattern comportamentali
- contrastare le strategie di propaganda con strategie altrettanto sofisticate

1 Il WEB 3.0 e l'approccio semantico

Come prevenire/arginare il danno derivante da un uso «doloso» dei social media?

Il concetto di «Web 3.0» è apparso la prima volta agli inizi del 2006:

- come estensione del web collaborativo;
- con lo scopo di associare, correlare, aggregare le informazioni ed i dati in formati adatti all'interrogazione e all'interpretazione



- **Metadato:** specifica il contesto semantico in un formato adatto all'interrogazione;
- **Big Data:** indica raccolta di dati così estesa da richiedere tecnologie e metodi analitici specifici per l'estrazione di valore;
- **Open Data:** concettualmente simili a Big Data, con l'unica differenza di essere liberamente accessibili a chiunque.

CYBER SECURITY SERVICES

SERVIZI GESTITI

SERVICE PORTAL

THREAT INTELLIGENCE

Il servizio di Threat Intelligence, che prevede l'installazione di una sonda DPI (Deep Packet Inspection), è volto ad analizzare la rete del cliente e ad identificare attacchi mirati in corso (Data Breach Detection) effettuati tramite Malware, Botnet, APT (Advanced Persistent Threats), attività di Phishing e di furto di credenziali

EARLY WARNING

Il servizio di Early Warning è volto ad identificare, analizzare e notificare tempestivamente, le vulnerabilità dei sistemi, tramite bollettini contestualizzati allo scenario tecnologico e di business del cliente, per garantire un adeguato supporto alle decisioni per l'attivazione di patch management

CONFIGURATION BACKUP

Soluzione per il backup delle configurazioni di apparati network e security senza limiti di tipologia o vendor

MONITORING

Soluzione centralizzata di monitoraggio dello stato di salute e performance di network e sicurezza. Monitoraggio stato di siti, dispositivi, applicazioni, prestazioni banda, etc

SECURITY EVENT CORRELATION

Tramite il servizio SIEM è effettuata l'analisi e la correlazione in tempo reale di tutti i LOG prodotti dai dispositivi e software monitorati, per rilevare in maniera tempestiva attacchi mirati (Security Event Management) e violazioni dei dati (Security Information Management)

DIGITAL SURVEILLANCE

Servizio innovativo che ha come obiettivo la ricerca di dati sensibili aziendali nella darknet per evitare compromissioni



Fabrizio De Santis

fabrizio.desantis@business-e.it

www.business-e.it

AN ITWAY GROUP COMPANY

ITALY, FRANCE, SPAIN, PORTUGAL, GREECE, TURKEY, U.A.E.
Ravenna, Milano, Trento, Massa, Roma, Bari, Vicenza, Paris, Barcelona,
Madrid, Lisboa, Athina, Istanbul, Ankara, Dubai-Hamiryah-Sharja