Cybercrimes: ICT e attività criminali

Prof. Avv. Roberto De Vita
Direttore Osservatorio IT e Sicurezza
Eurispes

Sole 24 Ore Master
Criminologia e Reati Economici

Milano, 1 – 2 Aprile 2016

Cybercrime: Italia

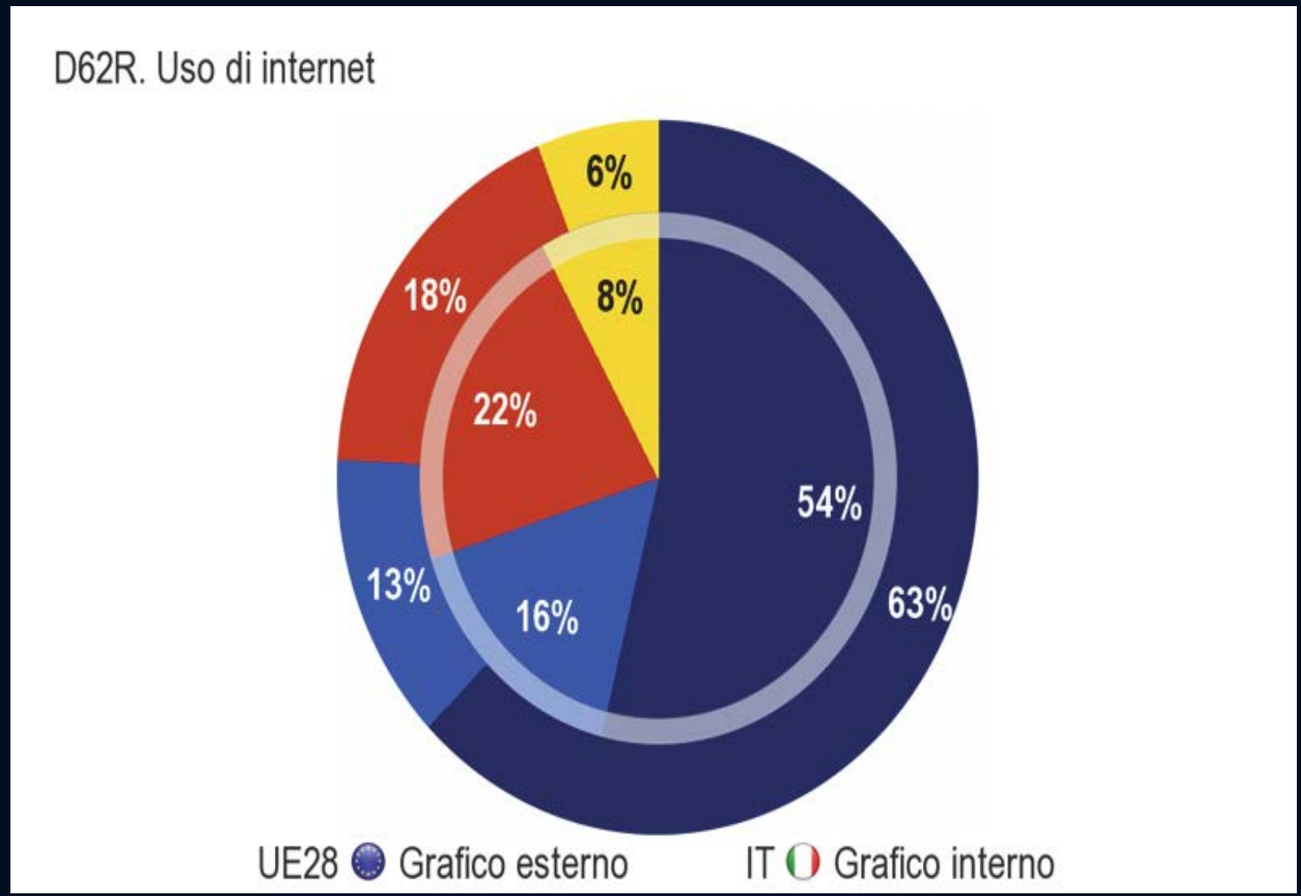
Sessione 3

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

Italia e Internet

- 54% utilizza internet quotidianamente
- 16% utilizza internet spesso
- 22% non lo utilizza mai
- 8% non ha accesso a internet

(Rapporto Eurobarometro Italia 2015)



Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

Italia e Internet

Dispositivi utilizzati per accedere

- Computer
- Smartphone
- Tablet e touch screen
- TV

Attività svolte online

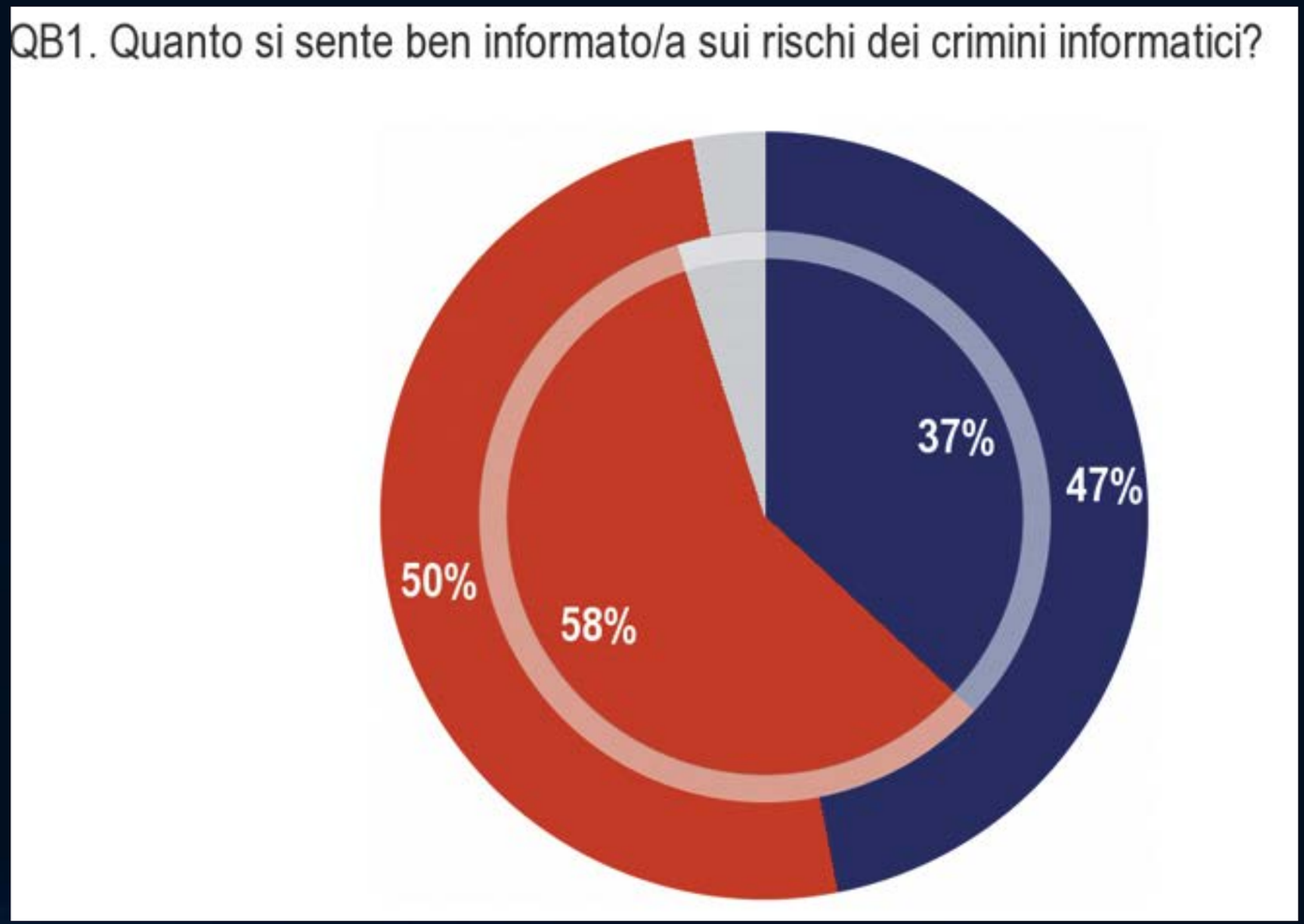
- Accesso e-mail (81%)
- Lettura notizie online (64%)
- Social network (63%)
- Operazioni bancarie (38%)
- Acquisto beni/servizi (32%)
- Giochi online (30%)
- Guardare tv (9%)
- Vendita beni servizi (8%)

(Rapporto Eurobarometro Italia 2015)

ITALIA E CYBERCRIME

- **Consapevolezza del cybercrime**
  - ✓ **Solo il 37% si ritiene bene informato sui rischi del cybercrime**

(Rapporto Eurobarometro Italia 2015)

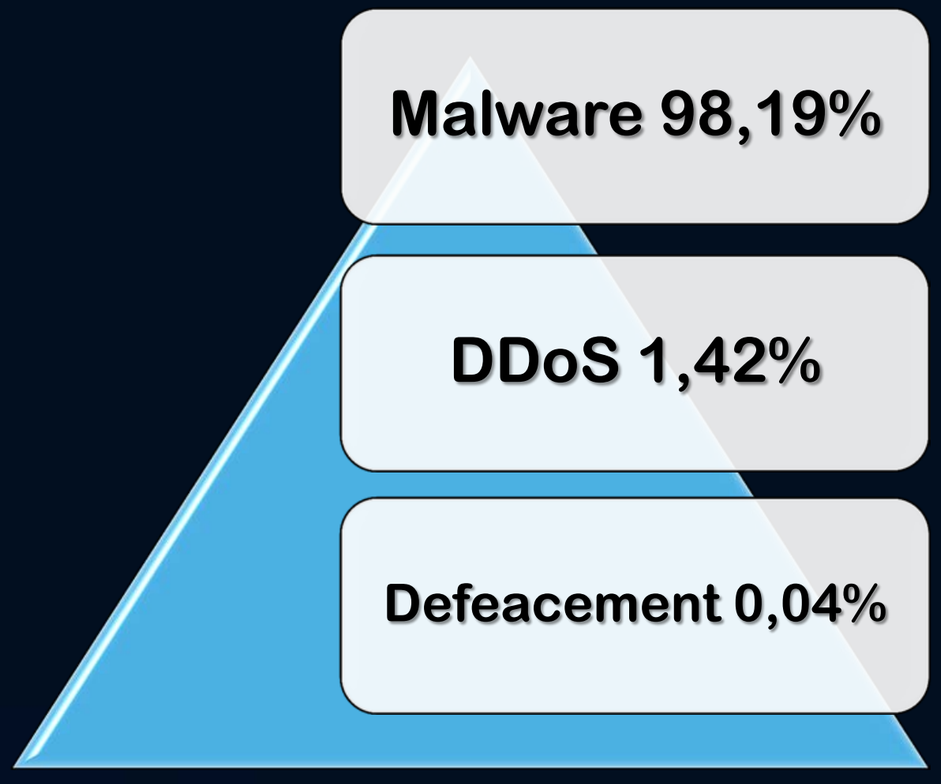


Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

ITALIA E CYBERCRIME

- ✓ Malgrado il mercato ICT sia in crescita il livello di cyber sicurezza in Italia stenta ad adeguarsi al costante aumento di episodi di cybercrime
- ✓ Anche le aziende non si adeguano ancora del tutto alle esigenze di ICT interna
- ✓ Nel 2015, le maggiori minacce in Italia giungono da malware utilizzati per furto di informazioni sensibili, monitoraggio delle azioni dell'utente, codifica dei dati con l'intento di estorcere denaro e/o partecipazione alla formazione di botnet

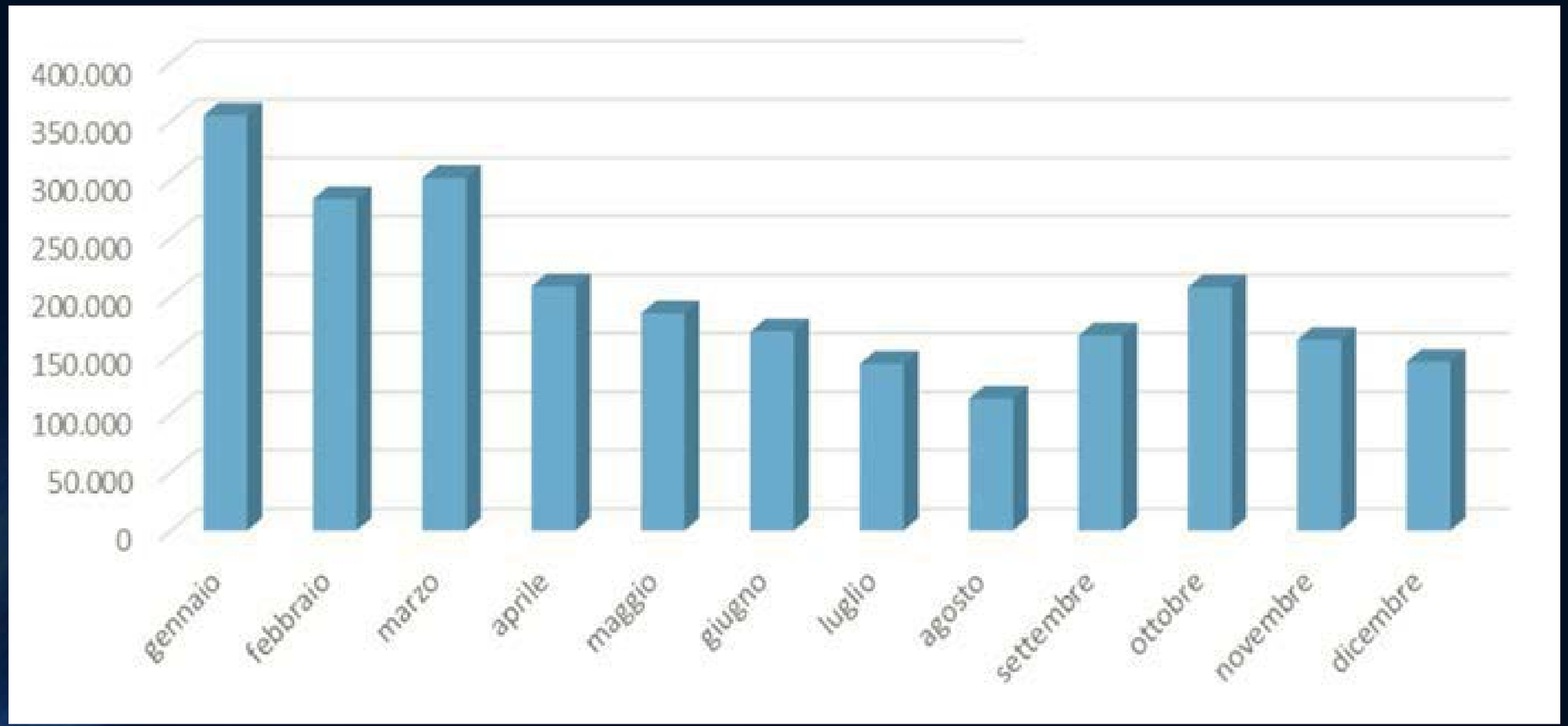
Top 3 tecniche di cyber attacco – Italia 2015:



(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

ITALIA E CYBERCRIME

Andamento temporale della diffusione dei malware



(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

ITALIA E CYBERCRIME

Gli attacchi DDOS

Diminuzione della durata degli attacchi

Record di attacchi DDOS nel 2015

Principali obiettivi :

aziende private (74%)

istituzioni (16%)

e

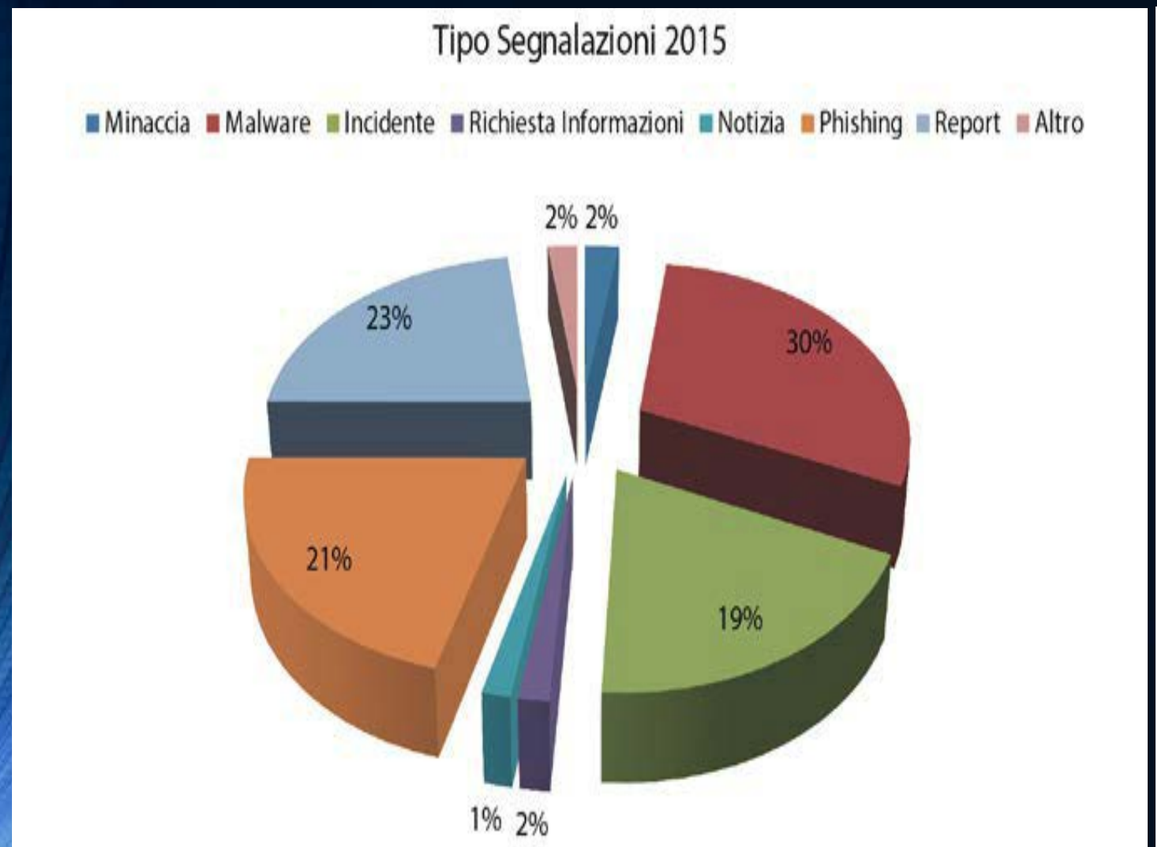
settore bancario (10%)

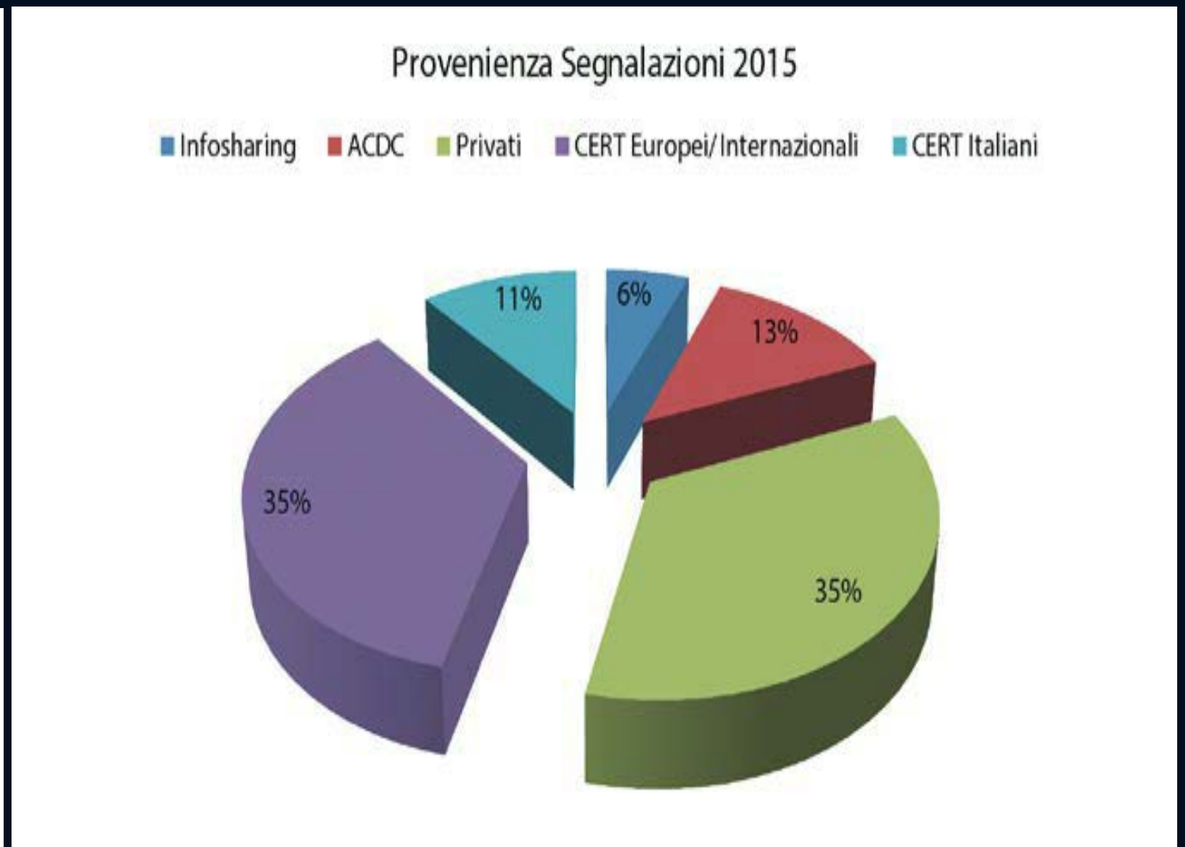
Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

ITALIA E CYBERCRIME

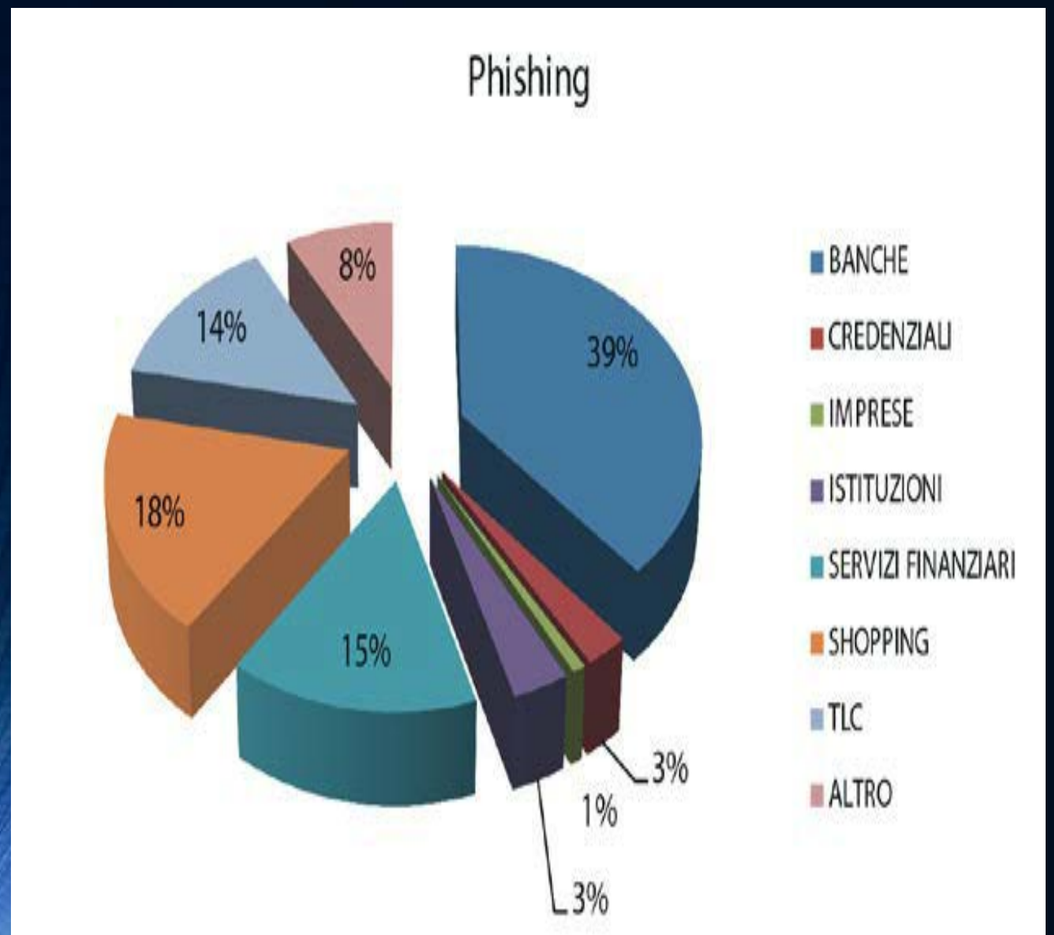
Le segnalazioni del CERT nazionale





(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

ITALIA E CYBERCRIME



Segnalazioni CERT nazionale - Phishing

- Le mail di Phishing continuano a rappresentare una delle principali minacce alla sicurezza delle reti
- Segnalazioni principali da omologhi CERT internazionali o *security vendors*
- I settori bancario e servizi finanziari, sono quelli per i quali è stato fatto ricorso maggiormente al CERT nazionale per ottenere supporto

(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

BUONE PRATICHE DI TUTELA

Phishing

- Fare backup periodici dei propri dati
- Diffidare da email inattese, specie se invitano ad aprire dei link
- Attivare sull'antivirus la funzione di navigazione sicura e verifica dei link
- Ridurre la superficie di attacco verificando periodicamente i plug-in installati all'interno di tutti i browser
- Accedere alle aree di memorizzazione in cloud solo per il tempo strettamente necessario
- Segnalare sempre attraverso gli appositi strumenti eventuali anomalie ovvero segnali di phishing o altri attacchi

(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

Italia e Cybercrime

Aree rilevanti per la sicurezza ICT in Italia

- Assicurazione del rischio informatico
- E-Commerce
- Furto di credenziali e fattori di rischio per le aziende italiane
- Sicurezza Informatica e prevenzione aziendale
- Sicurezza dei database
- Prospettive per la Mobile Security

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

TENDENZE FUTURE

Maggiore rilevanza dei social network nelle condotte di cybercrime

Aumento delle frodi su POS

Aumento domanda strumenti assicurativi contro «cyber-rischi»

Tendenza ad orientare gli attacchi sempre più verso device mobili (smartphone, tablet)

Estensione ransomware verso PA e Infrastrutture Critiche

(Rapporto Clusit sulla Sicurezza ICT in Italia – 2016)

FENOMENI : IL CYBER-LAUNDERING

Riciclaggio: operazioni volte a dare parvenza lecita a capitali di provenienza illecita. Sanzioni nel Codice Penale: art. 648-*bis*, 648-*ter* e 648-*ter.*1

Tre fasi:

FENOMENI : IL CYBER-LAUNDERING

La diffusione delle condotte di cybercrime ha determinato un costante aumento dell'utilizzo di mezzi informatici nelle condotte di riciclaggio:

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

MODALITÀ DI CYBER-LAUNDERING: MONEY TRANSFER

- ✓ Rappresenta la modalità più comune per il **cyber laundering**
- ✓ Tali servizi non richiedono procedure complesse per il trasferimento di fondi
- ✓ Spesso lo schema prevede trasferimento di fondi ai **money mules**, i quali prelevano le somme per poi inviarle al beneficiario tramite **money transfer**

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

MODALITÀ DI CYBER-LAUNDERING: SERVIZI DI PAGAMENTO ONLINE (IPS)

Strumento di pagamento riferibile a un conto bancario ma che funziona sfruttando la rete → permette di svolgere operazioni bancarie (a volte) in modo anonimo:

Denaro illegale trasferito su conto dei «money mules»

Prelievo e acquisto di «credit voucher» di un IPS

Comunicazione del voucher all'interessato che può utilizzarlo per acquisti online

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CYBER-LAUNDERING: MONEY MULES

Si tratta di «financial agents», consapevoli o meno dell'illiceità della condotta; spesso reclutati tramite e-mail spam oppure veri e propri annunci lavorativi «falsi».

Ruolo :

- ✓ Aprire un conto bancario o rendere il proprio disponibile per ricevere fondi illeciti
- ✓ Trasferire i fondi secondo istruzioni
- ✓ A volte ricevono commissione in %

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

ALTRE MODALITÀ DI CYBER-LAUNDERING

- Sistemi bancari paralleli
- Moneta elettronica /digitale
- Acquisti su internet
- *Smuggling* (trasferimento dei fondi derivanti da cybercrime)
- *Loan Back* (prestito a sé stesso)
- *Mixing* (confusione di fondi leciti e illeciti, rende complessa distinzione)

FENOMENI: «*OPERAZIONE TRIANGLE*»

Maggio – Giugno 2015: «*Operazione Triangle*» → emesse 62 ordinanze di custodia cautelare per soggetti di diverse nazionalità (prevalentemente nigeriani e camerunensi) di cui 29 dalla Procura di Perugia, per associazione per delinquere, accesso abusivo a sistema informatico, sostituzione di persona aggravata, truffa, ricettazione etc..

L'operazione ha coinvolto, oltre alla Polizia di Stato italiana, le Polizie di Spagna, Polonia, Regno Unito, Belgio, Georgia, Turchia e Camerun e Eurojust, Europol e Interpol.

L'organizzazione criminale transnazionale colpita, tramite la tecnica del «man in the middle», era riuscita a sottrarre illecitamente ingenti somme di denaro, sfruttando i rapporti di credito e debito esistenti tra diversi soggetti, tra cui società.

FENOMENI: «*OPERAZIONE TRIANGLE*»

Individua-zione di soggetti con rapporti debito-credito

Assunzione dell'identità del creditore nelle comunica-zioni telematiche

Dirottamento delle e-mail del debitore alla casella del gruppo criminale

Richiesta di pagamento al debitore, il quale corrisponde secondo le istruzioni del gruppo

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

FENOMENI: OPERAZIONE «*J-WEB*»

Luglio 2015 – Operazione «J-WEB» Ad esito di complesse attività di indagine eseguite dai **Carabinieri del ROS – Reparto Anti Eversione**, è stata emessa una ordinanza di custodia cautelare nei confronti di alcuni soggetti (di cui due residenti in Italia) i quali hanno costituito una cellula terroristica riconducibile ad *Al – Qaida*.

I soggetti, che si proponevano il compimento di atti terroristici, operavano soprattutto tramite un sito web, denominato «*Ashaq Al Hur*» o «*I7Ur* » attivo, oltre che nella pubblicazione di materiale propagandistico, nella selezione, arruolamento e addestramento di nuovi seguaci.

FENOMENI: OPERAZIONE «*J-WEB 2*»

Novembre 2015 – Operazione «J-WEB 2» I Carabinieri del ROS – Reparto Anti Eversione, in collaborazione con altre forze di Polizia europee, hanno eseguito l'ordinanza emessa dal Tribunale di Roma che ha portato all'arresto di 17 soggetti in tutta Europa, accusati di associazione con finalità di terrorismo. L'organizzazione di modello Jihadista, con vertice in Norvegia e numerose cellule in tutta Europa, fondava la propria attività sulle comunicazioni virtuali, che garantivano interconnessione ed anonimato. Le indagini hanno evidenziato la centralità degli strumenti informatici, sede virtuale, mezzo di comunicazione dei membri, luogo di confronto e formazione e principale strumento di divulgazione*.

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

*Fonte Sole 24 Ore

STRATEGIE ITALIA

Legge 133/2012 – attribuisce al comparto intelligence nuove competenze in materia di protezione cibernetica e sicurezza informatica

D.L. 179/2012 (convertito in L. 17.12.2012 n. 221) – «Decreto Crescita 2.0» - Attuazione dei principi dell'Agenda Digitale Europea

DPCM 24 Gennaio 2013 – Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

STRATEGIE ITALIA

DPCM 24 Gennaio 2013 – Indirizzi per la protezione cibernetica e la sicurezza informatica nazionale

DPCM 27 Gennaio 2014 – Quadro strategico nazionale per la sicurezza dello spazio cibernetico

DPCM 27 Gennaio 2014 – Piano Nazionale per la protezione cibernetica e la sicurezza informatica

Strategie Italia

Piano Nazionale - indirizzi operativi:

- Potenziamento capacità intelligence, polizia e difesa civile e militare
- Potenziamento organizzazione e coordinamento tra soggetti pubblici e privati
- Diffusione cultura della sicurezza informatica; formazione e addestramento
- Cooperazione internazionale ed esercitazioni
- Operatività del Computer Emergency Response Team (CERT)

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

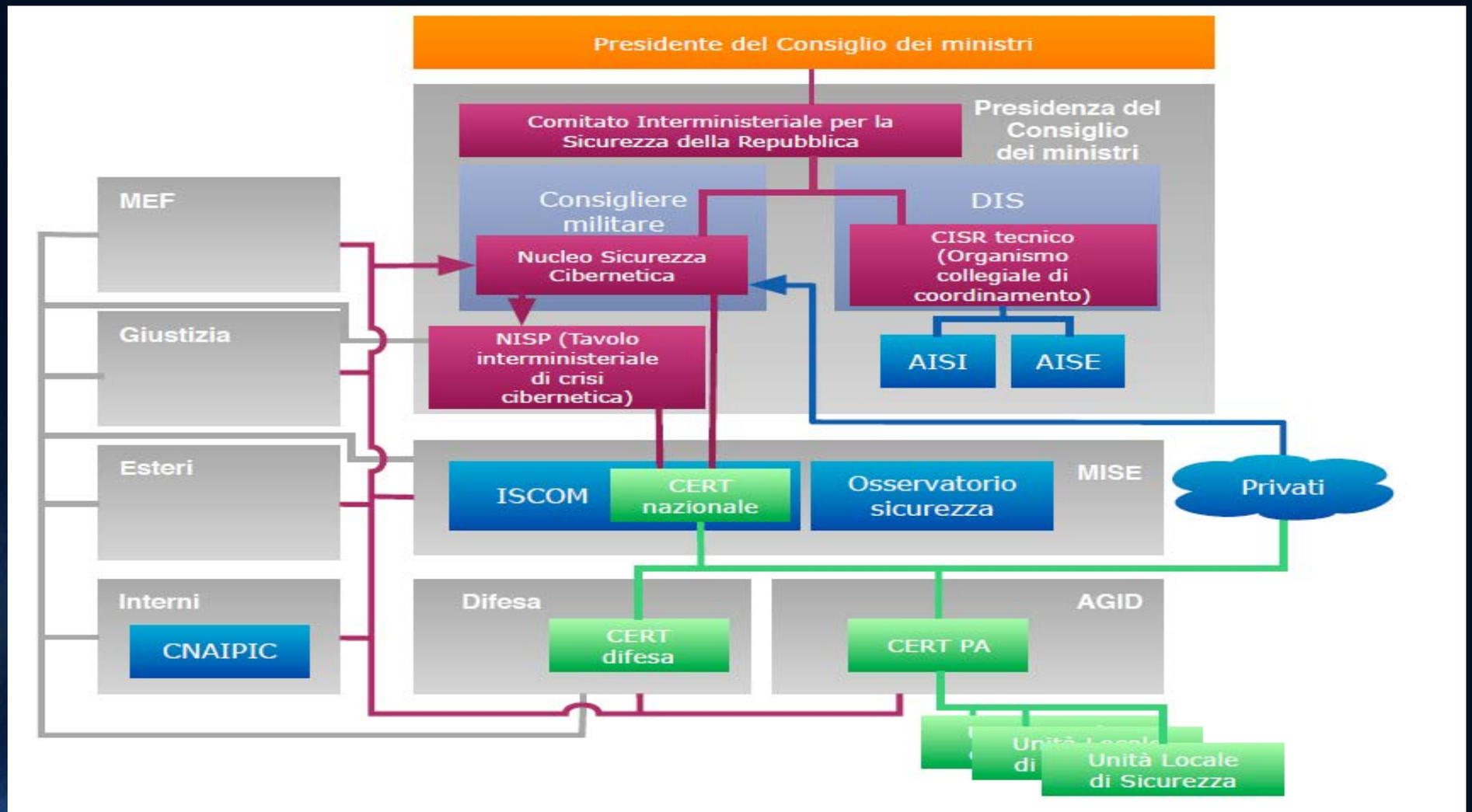
STRATEGIE ITALIA

Piano Nazionale – indirizzi operativi:

- Interventi legislativi e *compliance* con obblighi internazionali
- *Compliance* a *standard* e protocolli di sicurezza
- Supporto allo sviluppo industriale e tecnologico
- Comunicazione strategica
- Risorse
- Implementazione *Information Risk Management* nazionale

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CYBERCRIME: SOGGETTI OPERATIVI

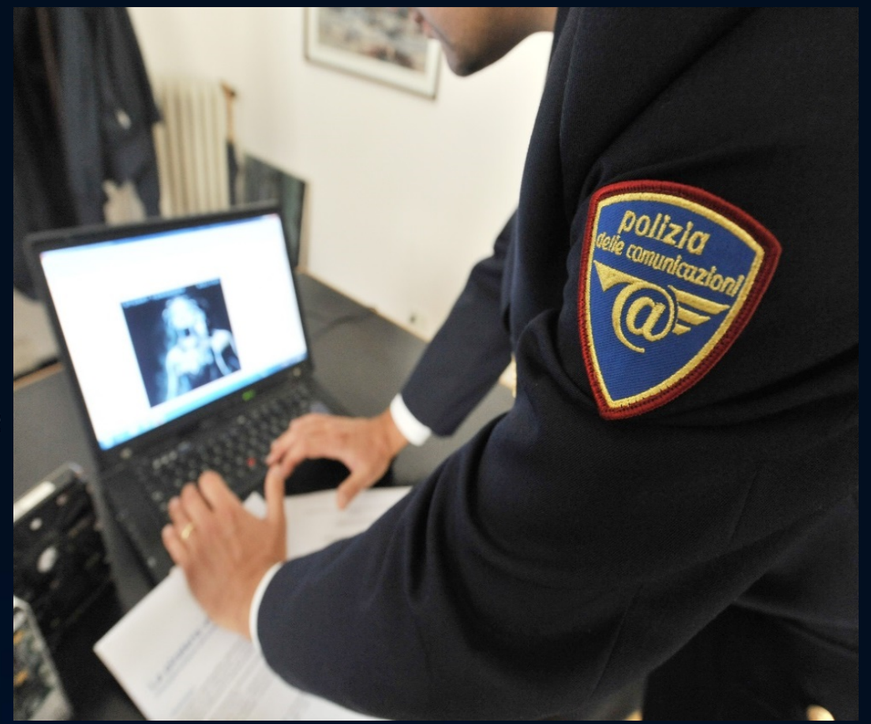


CONTRASTO AL CYBERCRIME

Polizia Postale e delle Comunicazioni:

- ✓ 20 compartimenti regionali e 80 sezioni territoriali, 2000 risorse con approfondite conoscenze informatiche
- ✓ 8 principali aree di intervento, per contrastare tutte le possibili aree di cybercriminalità:

  - Pedopornografia
  - Cyberterrorismo
  - Copyright
  - Hacking
  - Protezione delle Infrastrutture critiche del Paese
  - E-Banking
  - Analisi criminologica fenomeni emergenti
  - Giochi e scommesse online



Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CONTRASTO AL CYBERCRIME

Centro Nazionale Contrasto Pedopornografia Online

- Istituito presso il Servizio Polizia Postale e Comunicazioni del Dipartimento di Pubblica Sicurezza
- Punto di raccordo per segnalazioni di cittadini e Forze dell'Ordine
- Monitoraggio della rete per identificare spazi clandestini contenenti materiale pedo-pornografico
- Black List siti pedo-pornografici che viene fornita a Internet providers

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CONTRASTO AL CYBERCRIME

CNAIPC: Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche:

- ✓ Istituito con Decreto del Ministro dell'Interno 9.01.2008
- ✓ Prevenzione e contrasto della minaccia informatica di matrice terroristica o criminale
- ✓ Il CNAIPIC è inoltre il punto di contatto nazionale della Convenzione di Budapest sul Cybercrime e anche punto di contatto del Network 24/7 High Tech Crime del G8

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CONTRASTO AL CYBERCRIME

CNAIPC: Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche:

- Sezione investigativa composta da personale specializzato nel contrasto a cybercrime
- Sala operativa che eroga attività di prima risposta a cyber-emergenze
- Analisi dei dati
- Sezione tecnica a supporto delle attività operative

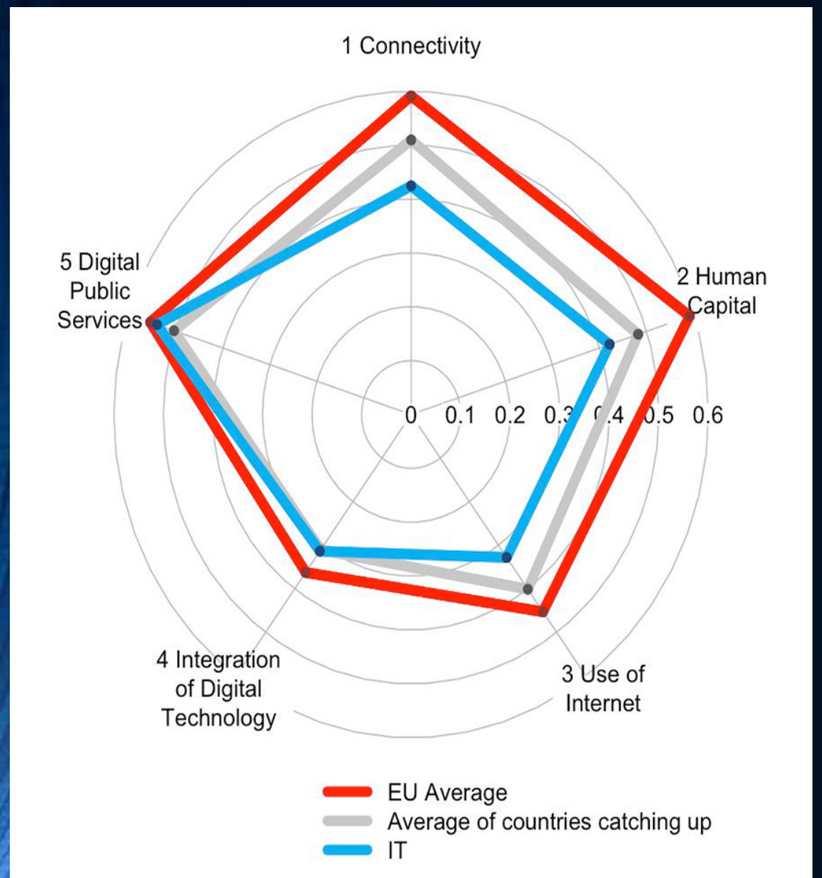
Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

CONTRASTO AL CYBERCRIME

CERT Italia: Computer Emergency Response Team

- Fornisce informazioni utili per la prevenzione e soluzione di crisi informatiche
- Fornisce informazioni volte alla sensibilizzazione sui temi di cybersecurity
- Fornisce supporto nella soluzione di crisi cibernetiche
- A livello internazionale, si interfaccia con i CERT delle altre nazioni e con quello europeo
- A livello nazionale, meccanismo di *infosharing* CERT-PA (il CERT della Pubblica Amministrazione), il CNAIPIC ed il CERT-Difesa.
- Dialogo a livello interno con le più grandi aziende di finanza, servizi, energia, etc.

DIGITALIZZAZIONE ITALIA



Digital Economy and Society Index (DESI)

- Indice composito elaborato dalla Commissione Europea per valutare lo stato di avanzamento degli Stati membri dell'UE verso un'economia e una società digitali.

- Risultati Italia DESI 2016:

  - ✓ Punteggio 0,4 (punteggio EU 0,52)
  - ✓ Posizione classifica n. 25
  - ✓ Pochi progressi in relazione a tutti gli indicatori, ad eccezione dell'e-commerce PMI
  - ✓ Il 37% della popolazione non usa internet regolarmente e il restante 63% svolge poche attività complesse online
  - ✓ L'Italia fa parte del gruppo di paesi che **stanno recuperando il ritardo**

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

DIGITALIZZAZIONE ITALIA

AGID: Agenzia per l'Italia Digitale

- Con DPCM dell'8.01.2014 è stato approvato lo Statuto dell'AGID

- Principali competenze e funzioni:

- ✓ Coordinamento informatico delle PPAA centrali e locali
- ✓ Emanazione di pareri interpretativi su disposizioni in materia di ICT
- ✓ Omogeneizzazione dei sistemi informativi pubblici
- ✓ Progettazione e coordinamento iniziative strategiche
- ✓ Vigilanza su qualità dei servizi e ottimizzazione della spesa
- ✓ Promozione dell'alfabetizzazione digitale
- ✓ Autorità di riferimento in ambito EU
- ✓ Realizzazione dell'Agenda digitale italiana ed europea
- ✓ Direzione e organizzazione attività del CERT
- ✓ Diffusione delle tecnologie digitali per crescita economica Italia secondo i pilastri dell'Agenda Digitale Europea

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

DIGITALIZZAZIONE ITALIA

AGID: Agenzia per l'Italia Digitale: Principali Obiettivi

- Progetto SPID (Sistema Pubblico per l'Identità Digitale)
- Piattaforma di comunicazione ed erogazione servizi per cittadini e imprese
- Supporto progetto ANPR (Anagrafe Nazionale della Popolazione Residente)
- Implementazione CERT PA
- Fatturazione elettronica PA
- Collaborare all'attuazione della Open Data Charter
- Piano strategico per la banda ultralarga e crescita digitale
- Sviluppo del sistema pubblico di connettività – SPC

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

DIGITALIZZAZIONE ITALIA

Strategia per la crescita digitale 2014-2020

- Parte della Strategia di crescita digitale e banda ultralarga nell'ambito dell'Agenda Digitale Italia
- Azioni per la crescita digitale:
  - ✓ Sistema pubblico di connettività e wi-fi per tutti gli edifici pubblici
  - ✓ Digital Security per la PA (aumentare il digitale per tutelare la privacy, l'integrità e la continuità dei servizi della PA)
  - ✓ Razionalizzazione del patrimonio ICT, consolidamento data center e cloud computing
  - ✓ SPID

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

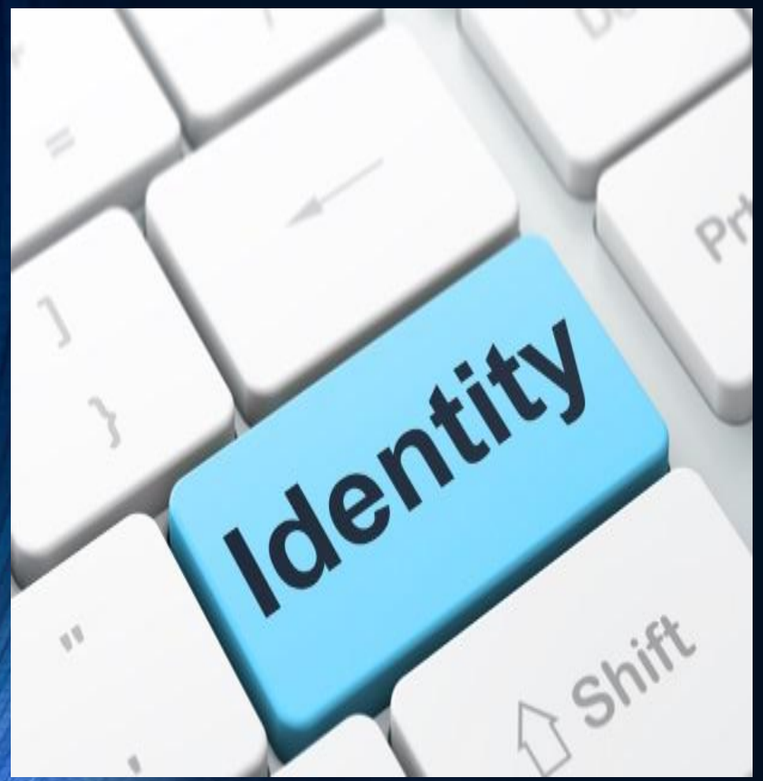
DIGITALIZZAZIONE ITALIA

SPID: Sistema Pubblico per l'Identità Digitale

- «Italia Log In» = nuovo modo digitale di relazionarsi fra PA e cittadini/imprese
- Accessi in rete ai servizi della PA (e ad alcuni servizi privati) mediante identità digitale
- **Ruoli:**
  - ✓ Identity Provider: forniscono le identità digitali e svolgono le attività di autenticazione
  - ✓ Service Provider: forniscono servizi digitali accessibili attraverso credenziali SPID
  - ✓ Attribute Provider: forniscono attributi qualificati quali attestazione di stati, ruoli, titoli e cariche

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

DIGITALIZZAZIONE ITALIA



SPID: Sistema Pubblico per l'Identità Digitale

- Marzo 2016: sono online i primi servizi accessibili tramite SPID
- Circa 300 servizi (una decina di PA) diventeranno 600 entro Giugno
- Entro 24 mesi è prevista l'adesione di tutta la PA
- L'AGID svolgerà funzione di regolatore e vigilanza sul sistema
- Il Governo ritiene che ci saranno 3 milioni di cittadini dotati di SPID entro fine 2016 e 10 milioni entro il 2017*

* Fonte Repubblica

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

Italia e Cybercrime

1993 – Legge 23 Dicembre 1993 n. 547 – Modificazioni ed integrazioni alle norme [...] in tema di criminalità informatica

2008 – Legge 18 Marzo 2008 n. 48 – Ratifica ed esecuzione della Convenzione di Budapest del 2001

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

ITALIA E CYBERCRIME

- **Art. 491-*bis* c.p. – Documenti informatici (introdotto nel 1993 e modificato nel 2008 e nel 2016*)**

  «Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti gli atti pubblici»

*(D. Lgs. 15.01.2016 n. 7)

ITALIA E CYBERCRIME

- **Art. 495-*bis* c.p. – Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri (introdotto nel 2008)**

«Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno»

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

ITALIA E CYBERCRIME

- **Art. 615-*ter* c.p. – Accesso abusivo ad un sistema informatico o telematico (introdotto nel1993)**

  «Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

  La pena è della reclusione da uno a cinque anni:

  1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita abusivamente la professione di investigatore privato o con abuso della qualità di operatore di sistema;
  2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;»…

ITALIA E CYBERCRIME

- **Art. 615-*ter* c.p. – Accesso abusivo ad un sistema informatico o telematico (introdotto nel 1993)**

  3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

  Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

  Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.»

ITALIA E CYBERCRIME

- **Art. 615-*quater* c.p. – Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (introdotto nel 1993)**

  «Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.

  La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'art. 617-*quater*»

ITALIA E CYBERCRIME

- **Art. 615-*quinquies* c.p. – Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (introdotto nel 1993 e modificato nel 2008)**

  «Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329»

ITALIA E CYBERCRIME

- **Art. 617-*quater* c.p. – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (introdotto nel 1993)**

  «Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.

  Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

  I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa»...

ITALIA E CYBERCRIME

- **Art. 617-*quater* c.p. – Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (introdotto nel 1993)**

  «Tuttavia si procede d`ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

  1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

  2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualita` di operatore del sistema;

  3) da chi esercita anche abusivamente la professione di investigatore privato»

ITALIA E CYBERCRIME

- **Art. 617-*quinquies* c.p. – Installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (introdotto nel 1993)**

  «Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni.

  La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater»

Italia e Cybercrime

- **Art. 617-*sexies* c.p. – Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (introdotto nel 1993)**

  «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

  La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater»

ITALIA E CYBERCRIME

- **Art. 621, comma 2, c.p. – Rivelazione del contenuto di documenti segreti (introdotto nel 1993)**

  «[…] Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi […]»

ITALIA E CYBERCRIME

- **Art. 635-*bis* c.p. – Danneggiamento di informazioni, dati e programmi informatici (introdotto nel 1993 e modificato nel 2008 e nel 2016*)**

  «Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni.

  Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni»

*(D. Lgs. 15.01.2016 n. 7)

ITALIA E CYBERCRIME

- **Art. 635-*ter* c.p. – Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (introdotto nel 2008 e modificato nel 2016*)**

  «Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

  Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni.

  Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata»

*(D. Lgs. 15.01.2016 n. 7)

ITALIA E CYBERCRIME

- **Art. 635-*quater* c.p. – Danneggiamento dì sistemi informatici o telematici (introdotto nel 2008 e modificato nel 2016*)**

  «Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.

  Se il fatto è commesso con violenza alla persona o con minaccio ovvero con abuso della qualità di operatore del sistema, la pena è aumentata»

*(D. Lgs. 15.01.2016 n. 7)

Prof. Avv. Roberto De Vita
Milano, 2 Aprile 2016

ITALIA E CYBERCRIME

- **Art. 635-*quinquies* c.p. – Danneggiamento di sistemi informatici o telematici di pubblica utilità (introdotto nel 2008 e modificato nel 2016*)**

  «Se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

  Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni.

  Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata»

  *(D. Lgs. 15.01.2016 n. 7)

ITALIA E CYBERCRIME

- **Art. 640-*ter* c.p. – Frode informatica (introdotto nel 1993 e modificato nel 2013)**

  «Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico e telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

  La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1 del secondo comma dell'art. 640, ovvero se il fatto è commesso con abuso della qualità di operatore di sistema»…

ITALIA E CYBERCRIME

- **Art. 640-*ter* c.p. – Frode informatica (introdotto nel 1993 e modificato nel 2013)**

  «La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.

  Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante»

ITALIA E CYBERCRIME

- **Art. 640-*quinquies* c.p. – Frode informatica del soggetto che presta servizi di certificazione di firma elettronica (introdotto nel 2008)**

  «Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro»

Italia e Cybercrime

- **D. Lgs. 8 Giugno 2001 n. 231 – Art. 24-*bis* – Delitti informatici e trattamento illecito dati (introdotto nel 2008)**

  «In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

  In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 615-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

  In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

  Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere a), b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere b) ed e). Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)»

ITALIA E CYBERCRIME

- **D. Lgs. 30 Giugno 2003 n. 196 – Art. 132, comma 4-*ter***

  «[…] Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi»

ITALIA E CYBERCRIME

- **D. Lgs. 30 Giugno 2003 n. 196 – Art. 132, comma 4-*quater***

  «Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-*ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente, l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale»[...]

Cybercrimes: ICT e attività criminali

Prof. Avv. Roberto De Vita
Direttore Osservatorio IT e Sicurezza
Eurispes

Sole 24 Ore Master
Criminologia e Reati Economici

Milano, 1 – 2 Aprile 2016