

# Sicurezza informatica e responsabilità sociale, l'importanza della consapevolezza

Andrea Zwirner

 andrea@linkspirit.it

 @AndreaZwirner

# Chi sono

- Mi interesso di sicurezza informatica dallo scorso millennio
  - “Connettere” significava “intrecciare”
  - Hacker non aveva ancora alcun significato
- Ho fondato Linkspirit, azienda che si occupa di
  - Consulenza nella progettazione sicura di software e sistemi
  - Verifiche di sicurezza su software e sistemi
  - Formazione in materia di sicurezza informatica

# Cosa faccio

- Partecipo a diversi progetti liberi legati la divulgazione della cultura sulla sicurezza informatica



[www.isecom.org](http://www.isecom.org)



[www.hackerhighschool.org](http://www.hackerhighschool.org)

Progetto scuole

[www.progettoscuole.it](http://www.progettoscuole.it)

Il problema non è tecnologico, ma culturale.

# Cos'è la sicurezza applicativa

- Comprende alcune questioni tecnologiche
- Consapevolezza di analisti, sviluppatori, tester, **utenti finali**
  - Sviluppo dell'architettura (secure by design)
  - Ciclo di sviluppo del software
  - Scrittura del codice
  - Controlli di sicurezza comuni nelle fasi di test / review
  - **Utilizzo consapevole da parte degli utenti finali**

# Qual è l'idea da cui dobbiamo liberarci



# In realtà le cose vanno così



# In realtà le cose vanno così

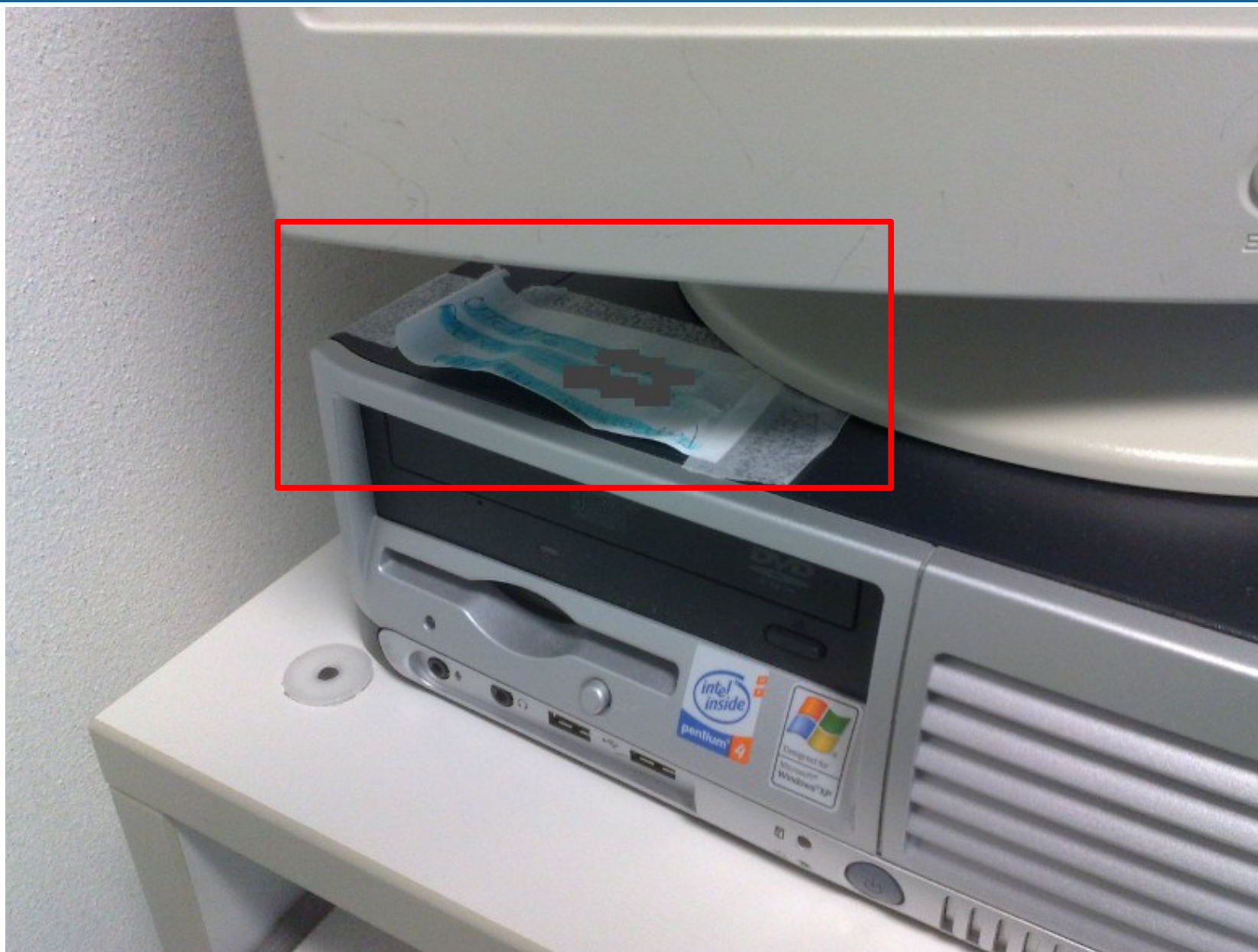




# In realtà le cose vanno così



# In realtà le cose vanno così



# Il problema della sicurezza è culturale

- Possiamo immaginare la sicurezza come una catena composta da anelli tecnologici ed umani
- Portare a buon fine un attacco informatico significa riuscire a rompere questa catena
- Una catena è resistente quanto il suo anello più debole
- L'anello più debole della catena è la componente umana

# Un esempio concreto: il phishing

- Viene attuato mediante messaggi privati
- Ha il fine di far decidere all'utente di compiere un'azione
  - visitare una pagina web all'utente per e portarlo ad inserire le proprie credenziali, rubandogliele
  - eseguire un software malevolo per prendendone il controllo della sua postazione
- Il messaggio può provenire da persone (o aziende) conosciute, facendo leva sulla fiducia che l'utente ripone in queste ultime
- Fa leva sulla curiosità dell'utente

# Un esempio di phishing



# Un esempio di phishing

www.zoya-interiors.com/slbz.php

**PayPal**

## Accedi al tuo conto

Indirizzo email

Password

**Accedi**

[Hai dimenticato l'indirizzo email o la password?](#)

**Registrati gratis**

**Scegli tu come pagare.**  
Paga con una delle tue carte o con il saldo PayPal. A te la scelta.

**Semplice. E in genere gratuito.**  
Aprire un conto PayPal è gratuito e non paghi tariffe quando fai acquisti, non importa come decidi di pagare.

# Riepilogando

- L'utente è convogliato verso un sito che sembra quello di PayPal
- L'utente inserisce le proprie credenziali in tutta tranquillità
- Le credenziali vengono salvate, quindi l'utente ignaro dell'accaduto viene rediretto sul sito reale
- La maggior parte delle volte, l'utente non si accorge di nulla!
- L'attacco fa leva sulla mal riposta fiducia

# Il caso phishing SDA

- Arriva una mail dal corriere SDA che avverte di un pacco in fermo deposito
- rimanda al sito [mysda24.info](http://mysda24.info) per il download dei moduli per il ritiro



# Il caso phishing SDA

SDA :: RICERCA SPEDIZIONI

Web

[SDA http://mysda24.info/e592828105fa1cd3de42add791733be2](http://mysda24.info/e592828105fa1cd3de42add791733be2)

CERCA

1984 - 2014 30 anni  
**SDA**  
EXPRESS COURIER  
Gruppo Posteitaliane

my SDA 2.0  
SCOPRILO ORA!

**NUOVO MYSDA 2.0**  
Il portale web ricco di funzionalità per gestire le tue spedizioni a 360 gradi.

CHI SIAMO | COME SPEDIRE | SERVIZI | STRUMENTI ONLINE | MYSDA 2.0 | SOLUZIONI TECNOLOGICHE | ASSISTENZA ONLINE | NEWS

20 novembre 2014 - Informazioni operative | Servizi Internazionali - Informazioni operative

**ASSISTENZA ON-LINE**

 **SCRIVI ORA**

Per spedizioni in corso, Prova di Consegna, e pratiche reclami

 **CONSULTA LE FAQ**

Le domande più comuni per spedire e ricevere.

ALTRI CANALI DI ASSISTENZA

**RICERCA SPEDIZIONI O TRACKING**

Per scaricare le informazioni sul vostro pacchetto si prega di inserire il numero mostrato nell'immagine qui sotto:

Il tracking on line (Ricerca Spedizioni) ti mostra dove si trova la tua spedizione e qual è il suo stato operativo. Nella maggior parte delle spedizioni il percorso prevede alcune tappe fondamentali, come il ritiro della merce presso il mittente, il transito nelle filiali e centri di smistamento, la consegna presso il destinatario, ecc.

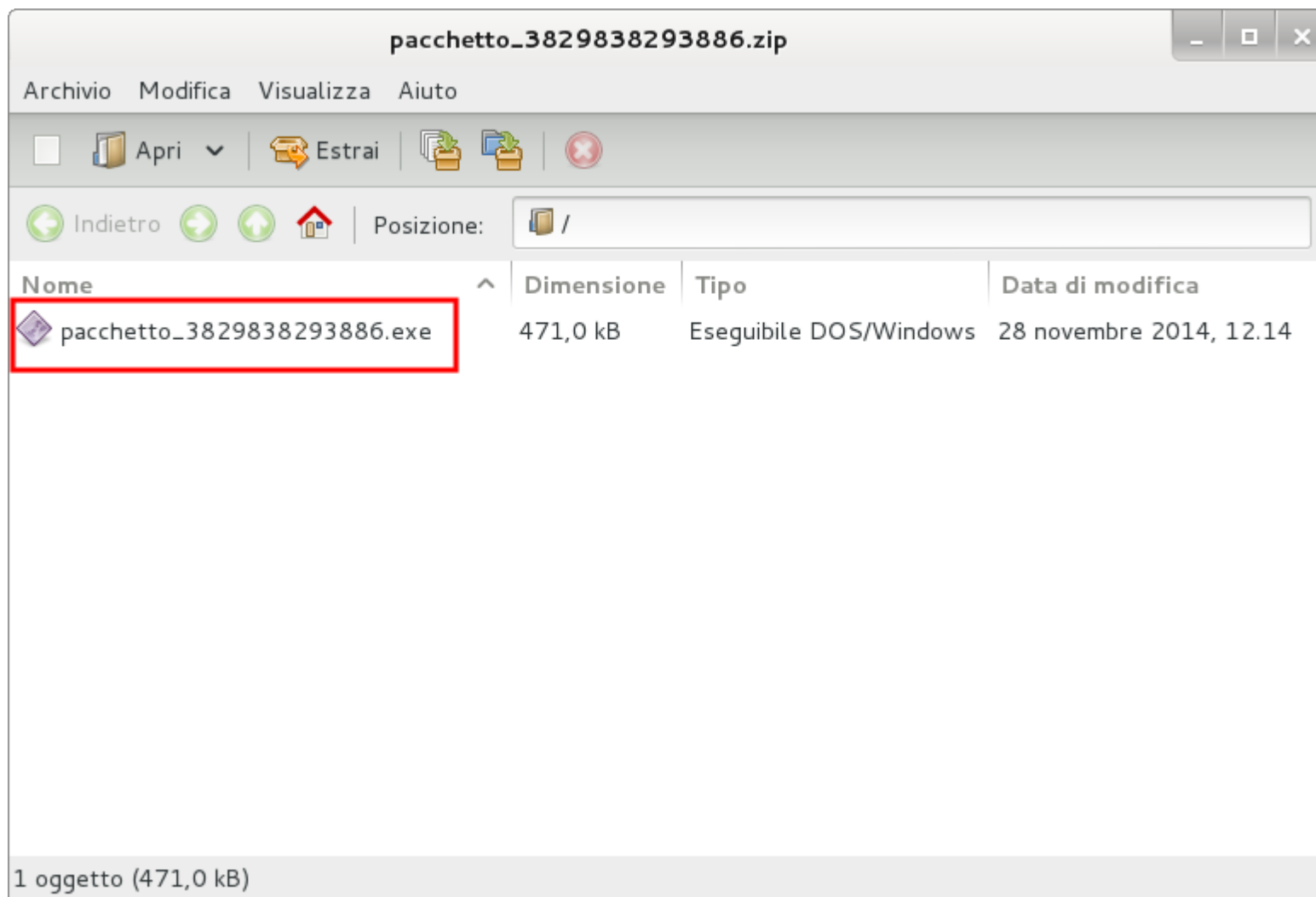
VUOI SPEDIRE CON SDA?

**AREA CLIENTI**

**ACCEDI**

my SDA 2.0 **NEW**

# Il caso phishing SDA



# Salvagente tecnologico

- E se l'utente ha un buon antivirus installato, aggiornato e perfettamente funzionante?

Il problema non è tecnologico, ma culturale.

# E se c'è un antivirus?

Browser address bar: <https://www.virustotal.com/it/file/9c417702b5b30ea8da88d81234d9b4e0f36974850a68383064ef38373ab3e1a7> DuckDuckGo

Navigation: Comunità Statistiche Documentazione FAQ Informazioni Italiano Entra nella nostra comunità Collegati


## virustotal

SHA256: 9c417702b5b30ea8da88d81234d9b4e0f36974850a68383064ef38373ab3e1a7

Nome del file: pacchetto\_382983829388.zip

Rapporto rilevamento: **4 / 56**

Data analisi: 2014-11-26 11:38:19 UTC ( 2 giorni, 3 ore fa ) [Leggi gli ultimi](#)



Analisi **Ulteriori informazioni** Commenti **1** Voti

Antivirus	Risultato	Aggiornamento
██████████	Generic_r.EHU	20141126
██████████	W32.HfsAutoA.5DA8	20141120
██████████	HEUR/QVM10.1.Malware.Gen	20141126
██████████	Suspicious.Cloud	20141126
██████████	✓	20141126
██████████	✓	20141121

# Gli antivirus non funzionano?

- Il modello di funzionamento degli antivirus oggi è obsoleto!
- La velocità di propagazione è troppo alta per permettere agli antivirus di essere efficaci!

# Antivirus is dead!

Symantec: Antivirus is 'DEAD' – no longer 'a moneymaker' • The Register

Web



http://www.theregister.co.uk/2014/05/06/symantec\_antivirus\_is\_dead\_and\_not\_a\_moneymaker/?mt=1417212730850



Log in | Sign up

Cash'n'Carrion | Whitepapers | The Channel

# The Register®

*Biting the hand that feeds IT*

Data Centre Software Networks **Security** Business Hardware Science Bootnotes Video Forums Weekend Edition

Search site



INTRODUCING  
F5 Silverline



Choose the most comprehensive  
L3-L7 DDoS solution in the cloud.

FIND OUT MORE



SECURITY

## Symantec: Antivirus is 'DEAD' – no longer 'a moneymaker'

**Oh, and it's still 40 per cent of our business**

By Iain Thomson, 6 May 2014



2,286 followers

[Linux and AIX Bare-Metal Recovery Webinar](#)

82

RELATED  
STORIES

Symantec, a company that has made huge amounts of cash as the largest antivirus software vendor for the last quarter of a century, looks to be getting out of that business and into fixing hacking problems rather than stopping them.

"We don't think of antivirus as a moneymaker in any way," Brian Dye, Symantec's

MOST READ

MOST COMMENTED

Ten excellent FREE PC apps to brighten your Windows

Tough Banana Pi: a Raspberry Pi for colour-blind diehards

Pity the poor Windows developer: The tools for desktop development are in disarray

Ten Mac freeware apps for your new Apple baby

Chromecast video on UK, Euro TVs hertz so badly it makes us judder – but Google 'won't fix'

SPOTLIGHT

# L'effetto degli attacchi di phishing

- Primo esempio
  - Furto di credenziali d'accesso, non a scopo collezionistico
- Secondo esempio
  - Controllo totale della postazione attaccata
    - Farvi transitare operazioni illecite
    - Usarla come base per sferrare altri attacchi informatici (verso l'interno o verso l'esterno)
    - Rubare dati aziendali
    - Rubare dati personali ed identità



# Cosa fare con un'identità rubata?

- Riciclare denaro sporco mediante il gioco on-line
  - Bastano due codici fiscali: uno perde l'altro vince!
  - Ma chi perde, i soldi dove li ha presi?
- Effettuare furti, ricatti, estorsioni,
  - ai danni dell'utente
  - ai danni di terzi
- La vittima spesso si trova imputata di reati compiuti a suo nome!

# Furto di identità

The screenshot shows the Rai 3 website interface. At the top, the word "REPORT" is displayed in large, stylized letters. To the right is the Rai 3 logo. Below the header, there is a navigation bar with links: HOME, PUNTATE, IL PROGRAMMA, CHI SIAMO, RASSEGNA STAMPA, VIDEO, ACQUISTO PUNTATE, NEWSLETTER, and SCRIVI. A search bar is located on the right side of the navigation bar.

The main content area features a large heading "PUNTATA DEL 28/10/2013" and a sub-heading "TI RUBO L'IDENTITÀ" in red. Below this, it says "DI GIUSEPPE LAGANÀ - Società". There is a "Mi piace" button with a Facebook icon and a "ShareThis" button with various social media icons.

A video player is embedded in the main content area, showing a woman in a red dress speaking. The Rai 3 logo is visible in the top right corner of the video player.

On the right side of the page, there is an "ARCHIVIO" section with the sub-heading "Inchieste on line:". Below this, there is a list of links: Puntate, Perché?, Com'è andata a finire?, C'è chi dice no, Anteprema, Goodnews, A confronto, L'emendamento, Extra, and Il prezzo e il valore.

Below the "ARCHIVIO" section is a "Ricerca avanzata:" section with several dropdown menus for "Stagione", "Servizio", "Argomento", and "Autore", and a "Cerca" button.

At the bottom right, there is a small thumbnail for a reportage by Milena Gabanelli titled "LA VITTORIA A TUTTI I COSTI" featuring an image of an elderly man.

# Il problema è culturale

- Perché gli attacchi visti vanno a buon fine?
- Perché gli utenti ripongono la loro fiducia nell'attaccante?
  - Perché si trovano in un luogo familiare e confortevole
  - Perché non conoscono i rischi cui sono esposti
  - Perché non sanno quanto sia facile portare a termine un attacco verso di loro e quanto gravi possano essere gli impatti

# La responsabilità sociale

- L'interconnessione globale facilita
  - l'informazione
  - le comunicazioni private e d'impresa
  - la proliferazione di software malevolo

# La responsabilità sociale

- Ogni volta che mi metto a rischio su Internet, metto a rischio tutte le persone che mi sono vicine
- Come posso evitare di mettermi a rischio se non sono consapevole di quali siano i rischi?
- La consapevolezza dei rischi di Internet è una questione di responsabilità sociale

# Il rischio per le PMI

- Tutti gli impiegati hanno accesso ad un computer
- Tutti i computer sono collegati ad Internet
- Tutti gli impiegati rivestono tutte le mansioni (o quasi)

# Il rischio per le PMI

- Nessun impiegato ha una preparazione adeguata ad affrontare le tematiche di sicurezza
- Cosa succede se
  - Serve un “programmino” per...
  - Si trova una chiavetta USB nel parcheggio?
  - In casella c'è un avviso di “pacco in fermo deposito”?
  - Arriva via email una “fattura da pagare”?
  - ...

# Il rischio per le PMI

- Le PMI costituiscono la maggior parte dell'economia e delle industrie europee e contribuiscono fino all'80% all'occupazione di alcuni settori industriali.
- La consapevolezza dei rischi Internet da parte degli utenti finali diventa una questione fondamentale per proteggerle



# Il rischio per le PMI

- Le PMI costituiscono la maggior parte dell'economia e delle industrie europee e contribuiscono fino all'80% all'occupazione di alcuni settori industriali.
- La consapevolezza dei rischi Internet da parte degli utenti finali diventa una questione fondamentale per proteggerle
- Spesso le grandi imprese ereditano molte delle problematiche delle PMI...

# La strategia europea



HIGH REPRESENTATIVE OF THE  
EUROPEAN UNION FOR  
FOREIGN AFFAIRS AND  
SECURITY POLICY

Brussels, 7.2.2013  
JOIN(2013) 1 final

**JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL,  
THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE  
COMMITTEE OF THE REGIONS**

**Cybersecurity Strategy of the European Union:**

**An Open, Safe and Secure Cyberspace**

## Se non si coinvolgono gli utenti, ogni sforzo è vano

*“Ensuring cybersecurity is a common responsibility. End users play a crucial role in ensuring the security of networks and information systems: they need to be made aware of the risks they face online and be empowered to take simple steps to guard against them.”*

Cybersecurity Strategy of the European Union  
Commissione europea, febbraio 2013

# La strategia italiana



# Consapevolezza

*“[...] al fine di rafforzare le capacità nazionali di prevenzione, reazione e ripristino [...] individua come nodi primari [...]:*

*promozione e diffusione della cultura della sicurezza cibernetica sia tra i cittadini che all'interno delle istituzioni [...] al fine di accrescere il livello di consapevolezza e di conoscenza della minaccia e dei relativi rischi”*

*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*

*Presidenza del Consiglio dei Ministri, dicembre 2013*

# Quindi, cosa dobbiamo fare?

- Il problema è ... ?

# Quindi, cosa dobbiamo fare?

- Il problema è **culturale** !
- Dobbiamo attivarci per arricchire la nostra base culturale
- E' essenziale che la consapevolezza dei rischi di Internet diventi parte della nostra cultura, sia personale che d'impresa

# Quindi, cosa dobbiamo fare?

- Come?



Grazie per l'attenzione.

# Sicurezza informatica e responsabilità sociale, l'importanza della consapevolezza

Andrea Zwirner

 andrea@linkspirit.it

 @AndreaZwirner