



AICA



UNIVERSITÀ
DEGLI STUDI
DI UDINE
hic sunt futura



DIDATTICA 2016
INFORMATICA
30^a EDIZIONE DEL CONVEGNO

La Cyber Security come competenza per l'innovazione

UNIVERSITÀ DEGLI STUDI DI UDINE

SCUOLA SUPERIORE

19 aprile 2016

<http://didamatica2016.uniud.it>

«Cyber Security nella
formazione e nella
didattica»

Carlo Muzzi
muzzi@acm.org

Abstract

Cyber Security nella formazione e nella didattica

Carlo Muzzi

AICA - Associazione Italiana per l'Informatica ed il Calcolo Automatico
muzzi@acm.org

Abstract. *La Cyber Security coinvolge ormai tutti gli aspetti della nostra esistenza digitale: la formazione e la didattica non possono utilizzare il ciber spazio ignorandone le minacce. Questo studio approfondisce alcuni scenari di rischio tipici nella formazione a distanza e nell'utilizzo del cloud tra docenti e discenti nell'era digitale, fornendo inoltre indicazioni sugli accorgimenti e sulle contromisure da adottarsi.*

Keywords: *Cyber Security, threats, e-learning, M-learning, cloud, privacy.*

«Cyber Security»: una definizione formale



The screenshot shows the top part of the ITU website. On the left is the ITU logo with the tagline "Committed to connecting the world". To the right is a search bar with the placeholder text "What would you like to search for?". Below this is a dark blue navigation bar with several menu items: "ITU", "General Secretariat", "Radiocommunication", "Standardization" (which is highlighted), "Development", "ITU Telecom", "Members' Zone", and "Join ITU". A secondary row of menu items includes "About ITU-T", "Study Groups", "Events", "All Groups", "Join ITU-T", "Standards", "Resources", "Workshops", and "Regional Presence".

YOU ARE HERE HOME > ITU-T > STUDY GROUPS > STUDY GROUP 17 > CYBERSECURITY

SHARE    

Definition of cybersecurity

Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability
- Integrity, which may include authenticity and non-repudiation
- Confidentiality

ITU is the United Nations specialized agency for information and communication technologies -ICTs.

ESTRATTO DA: <http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx>

«Cyber Security»: più in breve

cybersecurity 

noun | cy·ber·se·cu·ri·ty | \-si-,kyūr-ə-tē\

Definition of CYBERSECURITY

Popularity: Bottom 50% of words

measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

First Known Use of CYBERSECURITY

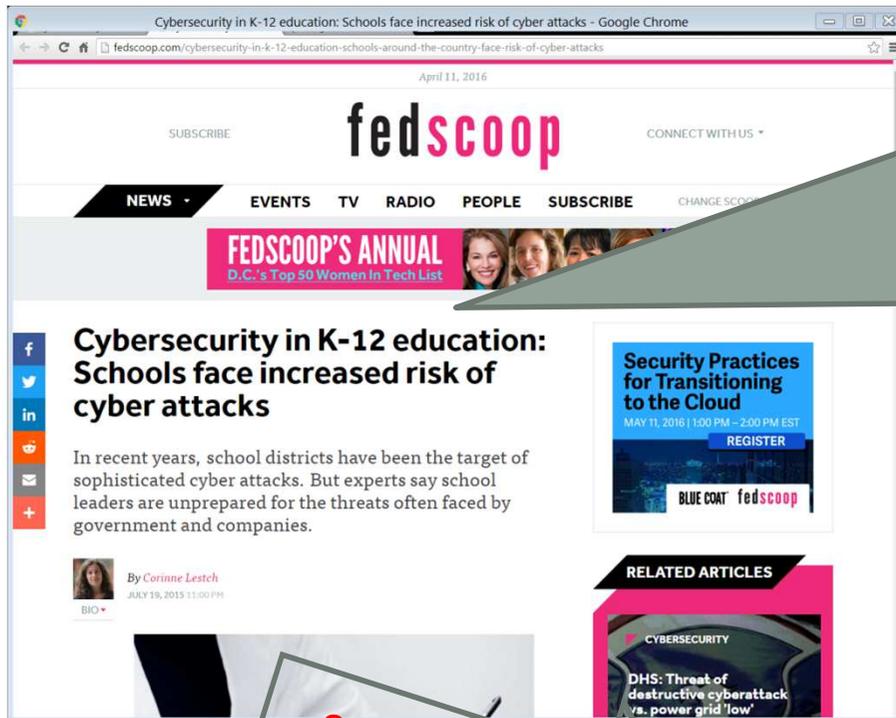
1994

1994



ESTRATTO DA: <http://www.merriam-webster.com/dictionary/cybersecurity>

Una minaccia avvenuta nella scuola USA



conseguenza

Gli alunni di 4 scuole elementari non hanno potuto accedere ai test programmati !

Terry Van Zoeren, sovrintendente in un distretto scolastico del New Jersey, racconta di una richiesta di riscatto per “sbloccare” i sistemi da un attacco ransomware.

Van Zoeren ricorda come, nei suoi 20 anni di carriera, mai avrebbe immaginato di avere a che fare con un attacco informatico.

ESTRATTO DA: <http://fedscope.com/cybersecurity-in-k-12-education-schools-around-the-country-face-risk-of-cyber-attacks>

Una minaccia avvenuta nella scuola italiana

Portale scuola Web – Attacco informatico

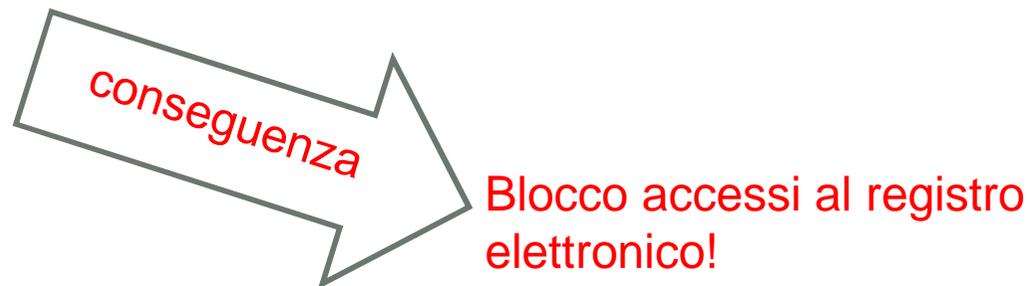
Si informano le SS.LL. che il gestore del portale Scuolaweb che ospita il registro elettronico scolastico ha segnalato che dalla giornata del 22 marzo è in atto un attacco informatico che ha costretto il gestore a bloccare l'accesso al sito e alle funzioni del registro stesso.

Si rammenta che i responsabili degli attacchi informatici potrebbero incorrere in conseguenze di tipo penale per interruzione di pubblico servizio nonché per danni economici. Qualora gli attacchi dovessero continuare, il gestore potrebbe valutare l'opportunità di inviare una segnalazione alla speciale sezione della Polizia postale, per l'effettuazione di indagini volte a tracciare gli attacchi per l'individuazione dei responsabili.

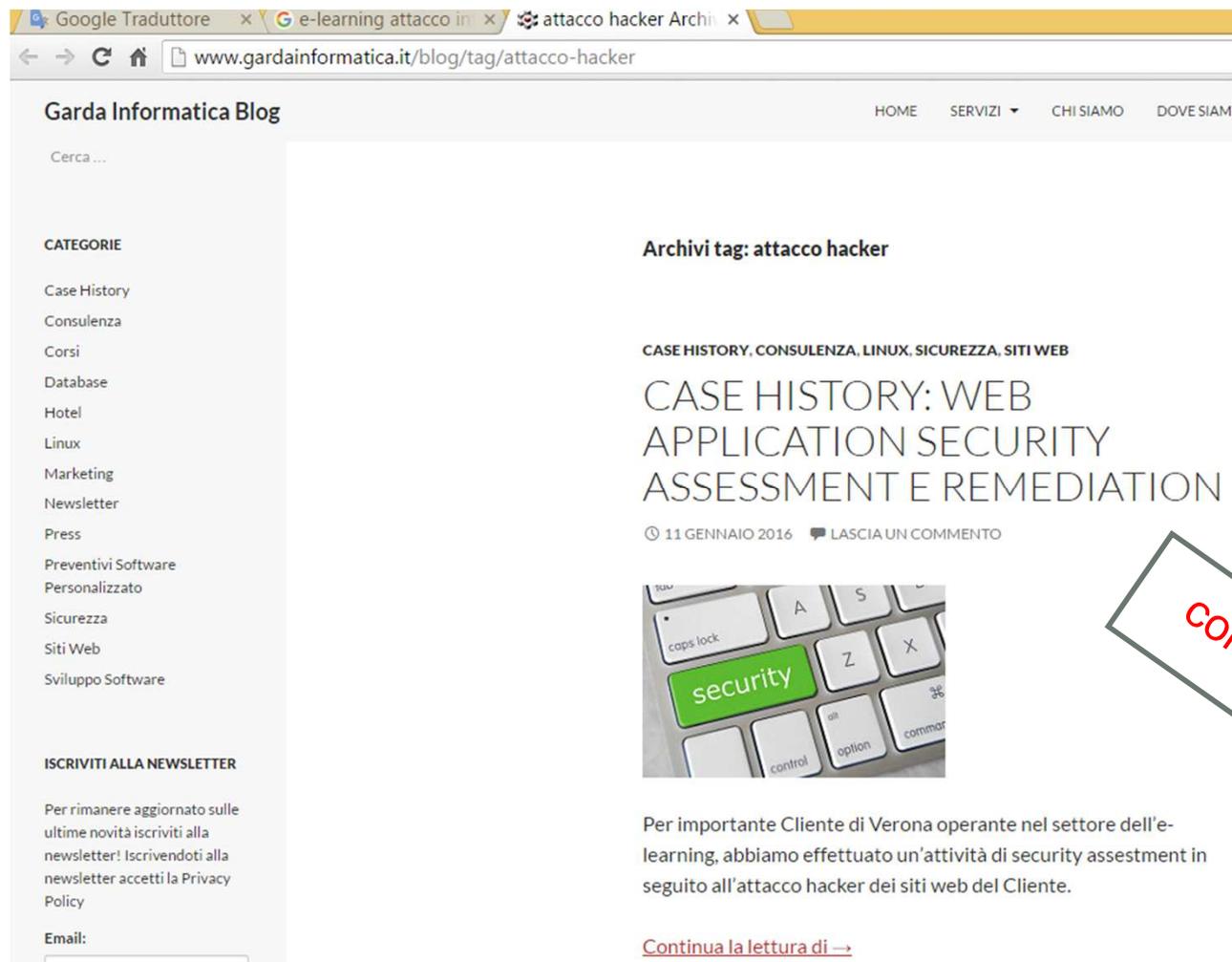
Si confida nella massima collaborazione da parte delle SS.LL.

Ringraziando per l'attenzione si porgono distinti saluti.

Il Dirigente Scolastico



Un caso nell' e-learning italiano



The screenshot shows a web browser window with the URL www.gardainformatica.it/blog/tag/attacco-hacker. The page title is "Garda Informatica Blog". The main content area displays a post titled "CASE HISTORY: WEB APPLICATION SECURITY ASSESSMENT E REMEDIATION" dated "11 GENNAIO 2016". The post includes a sub-header "Archivi tag: attacco hacker" and a list of categories: "CASE HISTORY, CONSULENZA, LINUX, SICUREZZA, SITI WEB". Below the title is a photograph of a computer keyboard with a green key labeled "security". The text of the post reads: "Per importante Cliente di Verona operante nel settore dell'e-learning, abbiamo effettuato un'attività di security assestment in seguito all'attacco hacker dei siti web del Cliente." A red arrow points from the text "consequenza" to the word "Non nota!".

Google Traduttore x e-learning attacco in x attacco hacker Archi x

← → ↻ 🏠 www.gardainformatica.it/blog/tag/attacco-hacker

Garda Informatica Blog HOME SERVIZI ▾ CHI SIAMO DOVE SIAMO

Cerca ...

CATEGORIE

- Case History
- Consulenza
- Corsi
- Database
- Hotel
- Linux
- Marketing
- Newsletter
- Press
- Preventivi Software
- Personalizzato
- Sicurezza
- Siti Web
- Sviluppo Software

ISCRIVITI ALLA NEWSLETTER

Per rimanere aggiornato sulle ultime novità iscriviti alla newsletter! Iscrivendoti alla newsletter accetti la Privacy Policy

Email:

Archivi tag: attacco hacker

CASE HISTORY, CONSULENZA, LINUX, SICUREZZA, SITI WEB

CASE HISTORY: WEB APPLICATION SECURITY ASSESSMENT E REMEDIATION

🕒 11 GENNAIO 2016 💬 LASCIA UN COMMENTO



Per importante Cliente di Verona operante nel settore dell'e-learning, abbiamo effettuato un'attività di security assestment in seguito all'attacco hacker dei siti web del Cliente.

[Continua la lettura di →](#)

consequenza

Non nota!

ESTRATTO DA: <http://www.gardainformatica.it/blog/tag/attacco-hacker/>

Gli attacchi ai siti (più tradizionali) colpiscono anche la scuola italiana

EDIZIONI ANSA > Mediterraneo Europa Nuova Europa Latina Brasil English Realestate

ANSA Toscana

Galleria Fotografica Video

CRONACA • POLITICA • ECONOMIA • SPORT • SPETTACOLO • IN VIAGGIO • SALUTE E CITTADINI • LA TUA ECON

ANSA.it • Toscana • **Attacco hacker islamista sito scuola**

Attacco hacker islamista sito scuola

In homepage un video dal titolo 'la verità prevarrà'

Redazione ANSA
FIRENZE
18 febbraio 2015
15:10
NEWS

Suggerisci
Facebook
Twitter
Google+
Altri
A+ A A-
Stampa
Scrivi alla redazione

Publicità 4w

Non restare in silenzio...
Milioni di bambini ogni giorno soffrono la fame!
Adotta ora



Attacco hacker islamista a sito istituto scuola Scandicci @ ANSA CLICCA PER INGRANDIRE

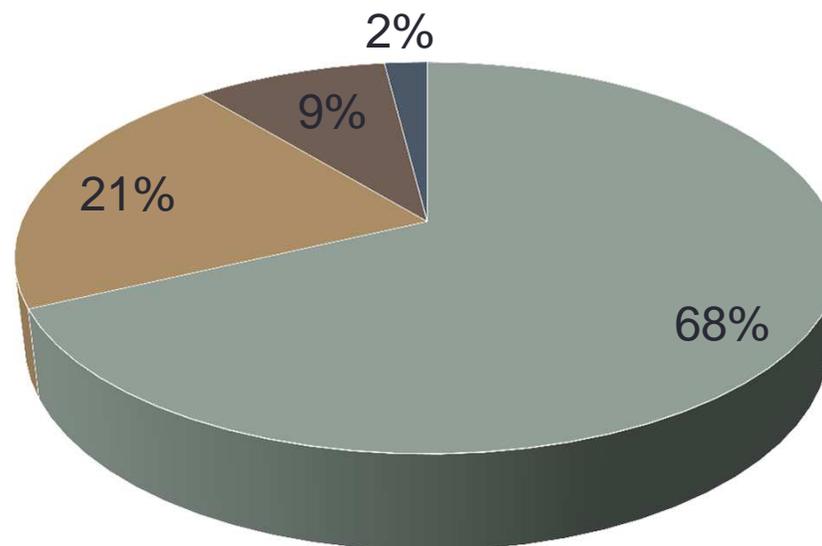
Attacco hacker islamista al sito di una scuola dell'hinterland fiorentino, l'istituto comprensivo di Scandicci (www.icscandicci.gov.it). Lo riferisce oggi il quotidiano La Nazione. Sono state cancellate tutte le informazioni sulla scuola e in prima pagina compare una schermata completamente nera con scritte rosse e bianche e un video 'the truth will prevail', la verità prevarrà. L'azione è firmata in home page da Moroccan Islamic Union Mail. Il video non mostra immagini cruente ma è annunciato da una scritta: "Non vogliamo mostrare i muscoli - scrivono gli hacker - vogliamo solo portare il messaggio in tutto il mondo per far scoprire la verità. E per il fatto che la si debba approfondire, ti invitiamo a guardare attentamente questo video per scoprire da solo quale è la verità". L'attacco è stato sferrato ieri e stamane la home page era ancora occupata dalla schermata nera della Moroccan Islamic Union Mail.

conseguenza

Si va oltre
l'inoperatività
del sito

ESTRATTO DA: http://www.ansa.it/toscana/notizie/2015/02/16/attacco-hacker-islamista-sito-scuola_c3f6335e-21ce-4453-a960-b9e2910c7080.html

La rete è una delle più grandi innovazioni della storia umana... ma porta anche rischi !



FONTE: Rapporto Clusit 2016
sulla Sicurezza ICT in Italia

- Cybercrime
- Hacktivism
- Spionaggio/Sabotaggio
- Guerra cibernetica

a) Tipologia e distribuzione degli attacchi nel 2015

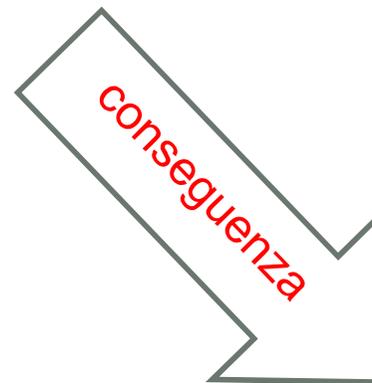
Dettaglio sul Cybercrime	2011	2012	2013	2014	2015	2012 su 2011	2013 su 2012	2014 su 2013	2015 su 2014	Trend 2015
	170	633	609	526	684	272,35%	-3,79%	-13,63%	30,04%	in aumento

b) L'attacco Cybercrime nel periodo 2011-2015

Minacce tecnologiche: i rischi per le piattaforme di e-learning

Le **piattaforme di e-learning** sostanzialmente prevedono:

- ❑ interfacce uomo macchina basate sul paradigma del browser;
- ❑ interazioni con front-end di siti e portali web;
- ❑ database per poter:
 - governare il processo di formazione (dinamico e adattivo per ogni discente)
 - profilare il discente ed il progresso di apprendimento
 - gestire il rapporto con l'utente con strumenti tradizionali (e-mail, chat, tutorial, ...) e social media (Facebook, YouTube, ...).



Sono esposte agli
stessi rischi delle
piattaforme web

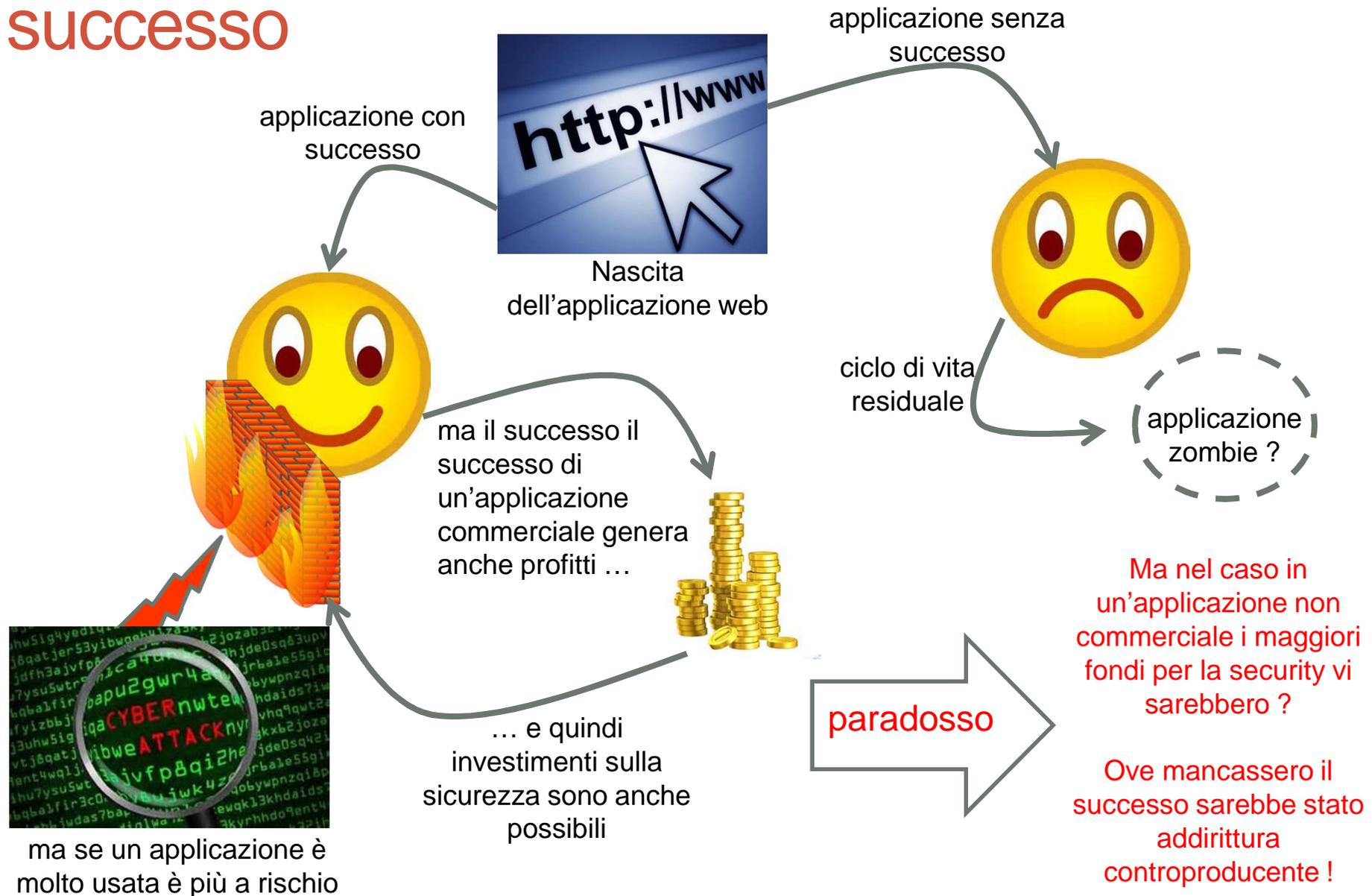
Minacce tecnologiche: i rischi per le piattaforme di e-learning

Minacce principali del 2015	Trend 2015
1- Malware (programmi malevoli)	in aumento
2- Attacchi web	in aumento
3- Attacchi ad applicazioni web	in aumento
4- Botnets (rete di dispositivi informatici infettati da malware controllati da remoto)	in diminuzione
5- Denial of service (negazione dei servizi)	in aumento
6- Danni fisici, furti o smarrimenti	stabile
7- Minacce interne (fraudolente e accidentali)	in aumento
8- Phishing (inganni via internet)	stabile
9- Spam	in diminuzione
10-Exploit kits (strumenti per eseguire attacchi informatici)	in aumento
11-Data breaches (violazione dei dati)	stabile
12-Furti di identità	stabile
13-Perdita di informazioni	in aumento
14-Ransomware (programmi che chiedono un riscatto per permettere l'accesso a documenti)	in aumento
15-Spionaggio cibernetico	in aumento

Panorama delle minacce cibernetiche del 2015

FONTE: European Union Agency For Network And Information Security), ENISA Threat Landscape 2015

Minacce tecnologiche: il paradosso del successo



Minacce tecnologiche: i rischi per le piattaforme di M-learning

Le piattaforme di **M-learning** rendono fruibile l'offerta formativa in ogni momento della vita quotidiana, perché si basano:

- ❑ sulla connettività in rete;
- ❑ sull'ausilio di dispositivi mobili:
 - PDA
 - Smartphone
 - Netbook

conseguenza

Sono esposte agli stessi rischi delle piattaforme web

+

... ma anche a quelli delle piattaforme mobile

Minacce tecnologiche: i rischi per le piattaforme di M-learning

Minacce principali del 2015	Trend 2015
1- Malware (programmi malevoli)	in aumento
2- Danni fisici, furti o smarrimenti	stabile
3- Attacchi ad applicazioni web	in aumento
4- Phishing (inganni via internet)	stabile
5- Attacchi web	in aumento
6- Perdita di informazioni	in aumento
7- Furti di identità	in aumento
8- Data breaches (violazione dei dati)	in aumento
9- Ransomware (programmi che chiedono un riscatto per permettere l'accesso a documenti)	in aumento
10-Botnets (rete di dispositivi informatici infettati da malware controllati da remoto)	in aumento

Minacce emergenti e trend nel Mobile Computing

Minacce tecnologiche: M-learning e il tema del BYOD

BYOD BRING YOUR OWN DEVICE



Gli sviluppi futuri: *Bring Your Own Device, e-learning e mobile learning*

Sempre in un'ottica di sostenibilità complessiva della Scuola Digitale, dato che è difficilmente pensabile il traguardo, per le Amministrazioni, di fornire un *device* a ciascun studente e a ciascun docente, è fondamentale che qualunque soluzione si voglia a mettere a disposizione della scuola (contenuti digitali, *cloud*, mercato elettronico) sia progettata con l'obiettivo di permettere agli studenti e ai docenti di utilizzare i propri *device* (*BYOD, Bring Your Own Device*), utilizzati quotidianamente (*smartphone, netbook, padfone ecc.*), ottenendo in tal modo un doppio vantaggio:

- sostenibilità economica, perché si usa quello che i ragazzi e i professori, spesso, possiedono già
- una scuola che permette e fa uso degli stessi strumenti di comunicazione utilizzati dai giovani, non può che aumentare il grado di coinvolgimento degli studenti.

Minacce tecnologiche: la proprietà nel BYOD

« ... essendo lo strumento utilizzato per la formazione **di proprietà dello studente e non della scuola**, anche se il soggetto formatore fosse in grado di applicare misure protettive o contenitive per erogare la didattica in sicurezza, quest'ultimo non potrebbe agire con autorità coercitiva ma dovrebbe limitarsi ad una sorta di moral suasion o, nel caso della formazione scolastica, con accordi parentali con quanti esercitano la patria potestà... »



Minacce tecnologiche: le soluzioni «pronte all'uso»

CMS OPEN SOURCE E-LEARNING

← → ↻ 🏠 https://www.google.it/?gws_rd=ssl#q=cms+open+so

Google

Tutti Notizie Immagini Video Shopping Altri

Circa 1.030.000 risultati (0,50 secondi)

LMS Open Source - Find Learning Management
[Ann](http://www.getapp.com/LMS) www.getapp.com/LMS ▼
 Save Time, See Reviews Now!
 Types: Open-Source, Free Trial, Enterprise, Small Business, Cloud
 a great way to get a first impression of an app – Business.com

Billing Software Top Scheduling Apps
 Project Management Apps Task Management Apps

Suggerimento: Cerca risultati solo in **italiano**. Puoi specificare la lingua di [Preferenze](#).

8 Best Open Source e-Learning CMS » CODECALL
codecall.net/.../8-best-open-source-e-learning-cms/ ▼ Traduci que
 16 mag 2014 - The 8 best open-source e-learning tools to take your class
 training to the next level. Integrate your current content or create robust new

Open Source e-Learning Scripts - OpenSourceCMS
www.opensourcecms.com/scripts/show.php?catid... ▼ Traduci ques
 A learning management system (LMS) is software for delivering, tracking,
 managing ... Moodle is a course management system (CMS) - a free, Open

Moodle - Open-source learning platform | Moodle.org
<https://moodle.org/?lang=it> ▼
 Moodle is a course management system (CMS) - a free Open Source software ...
 aperto e collaborativo di uno dei gruppi open source più grande al mondo.

Moodle - Open-source learning platform | Moodle.org
<https://moodle.org/> ▼ Traduci questa pagina
 Moodle is a course management system (CMS) - a free Open Source software
 package designed to help educators create effective online courses based on ...

Open Source e-learning for Business - Open Elms: e ...
www.openelms.org/ ▼ Traduci questa pagina

www.efrontlearning.net

efront

PRODUCT PARTNERS COMPANY BLOG SCHEDULE A DEMO

Make your talent thrive

Develop your people's skills and boost your business' value with a world-class Learning & Talent Development Platform

TAKE A TOUR PRIVATE CLOUD SOLUTIONS

[Moodle Pty Ltd \(AU\) https://moodle.org](http://Moodle Pty Ltd (AU) https://moodle.org)

DOCUMENTATION DOWNLOADS DEMO TRACKER DEVELOPMENT TRANSLATION MOODLE

Italiano (IT) Non sei ce

Guidato dalla community, supportato globalmente

Benvenuto nella community Moodle dove potrai scoprire il valore di un impegno aperto e collaborativo di uno dei gruppi open source più grande al mondo

COMMUNITY FORUMS

www.ilias.de/docu/ilias.php?ref_id=580&cmd=frameset&cmdClass=ilrepositorygui&cmdNode=n7&baseClass=ilrepositorygui

ILIAS

mas.de Using ILIAS

Using ILIAS
 Information about ILIAS, documentation, practice and add-ons

A Good Choice

There are a lot of reasons why public and private institutions and companies are already using ILIAS:

- A powerful system for web-based teaching and learning.
- A multi-purpose tool that can be used as a flexible course player, as an authoring tool, but also as a communication and collaboration platform.
- ILIAS is strongly respecting standards and was the first Open Source LMS that has been certified as SCORM 1.2 and SCORM 2004 compliant.
- ILIAS is open source software published under the General Public Licence and free of charge for every institution and organisation - no matter if 100 or 100 000 users are using the software.
- A secure LMS that has been certified by NATO and is allowed to be used in NATO's high security intranet.

ILIAS - the versatile software

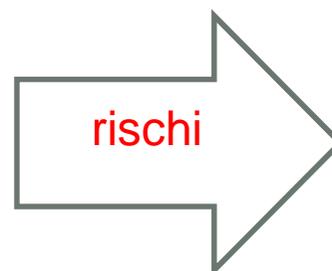
ILIAS - the well-engineered software

CERTIFIED
 SCORM® 2004
 Learning Management System

ILIAS allows not only to run SCORM 1.2 and SCORM 2004 modules successfully and according to both standards. ILIAS offers also an authoring environment to create SCORM 2004 learning modules online!

Minacce tecnologiche: i vantaggi dell'open source vanno gestiti

« ... Consideriamo ad esempio l'open source; è noto che la possibilità di disporre a vario titolo di software già realizzato da altri è una scelta generalmente seguita in molte organizzazioni: ma purtroppo questa scelta non introduce solo vantaggi, **vi sono anche elementi di rischio che vanno opportunamente gestiti** ... per gestirli occorre anche reinvestire una parte di quelle risorse risparmiate con l'utilizzo delle soluzioni aperte... »



**Risparmiare
anche sugli
investimenti in
sicurezza !**

Minacce tecnologiche: i vantaggi dell'open source vanno gestiti

Il nuovo
Regolamento
europeo per la
protezione dei
dati personali

- ❑ il Data Privacy Officer come attore proattivo della sicurezza
- ❑ Privacy by design
- ❑ Quadro regolatorio comune in Europa
- ❑ ...

conseguenza

Obbligherà a
rendere più
sicuro anche
l'open source

Minacce comportamentali

I comportamenti degli individui sono ormai generalmente accettati come fattori di rischio significativo per ogni attività umana che utilizza applicazioni informatiche:

- ❑ protezione delle **credenziali** di utilizzo dei sistemi → i rischi nella condivisione tra gruppi di individui di utenze e password
- ❑ **riservatezza dei contenuti e violazione dei diritti di terzi** → i rischi legali del cyberspazio
- ❑ **Cyberbullismo**
- ❑ **perdita di autorità o di controllo dello strumento tecnologico** da parte dei docenti → i rischi dei discenti «che ne sanno di più»

Minacce comportamentali: differenze generazionali

The screenshot shows the BitMat website header with a pink background. The logo 'BitMAT' is prominent on the left. To the right, there is a search bar with the text 'Cerca...' and a link 'Tv • Dossier on demand'. Below the search bar, there is a navigation menu with links: '> NEWS > TECNOLOGIE > INTERNET > MERCATI > APP > DEVICE > RUBRICHE >'. Below the navigation menu, there is a banner for 'RED 2016 Riviera Engineering Days' with a list of topics: 'ingegneria del turismo', 'agenda digitale', 'big data', 'smartgrid', 'efficienza energetica', 'creazione d'impresa', and 'cloud'.

BitMat » News

GIOVANI VS SENIOR: CHI SI PROTEGGE MEGLIO ONLINE?

Leggi più tardi



di Redazione BitMat

Gli over 45 anni sono più cauti dei giovani, ma non riconoscono le truffe. I giovani invece prendono meno precauzioni ma riconoscono le minacce

Kaspersky, sicurezza

12/1/2016

Quando si tratta di sicurezza online, gli utenti Internet di età uguale o superiore a 45 anni sono più cauti dei giovani nella condivisione di informazioni, ma potrebbero non essere in grado di riconoscere una truffa o una minaccia imminente. Secondo alcune recenti indagini sui consumatori* condotte da Kaspersky Lab, invece, gli utenti di età uguale o inferiore a 24 anni sono più disposti a rivelare informazioni personali online e prendono meno precauzioni per proteggersi, ma comprendono meglio le potenziali minacce e riescono a riconoscerle più facilmente.

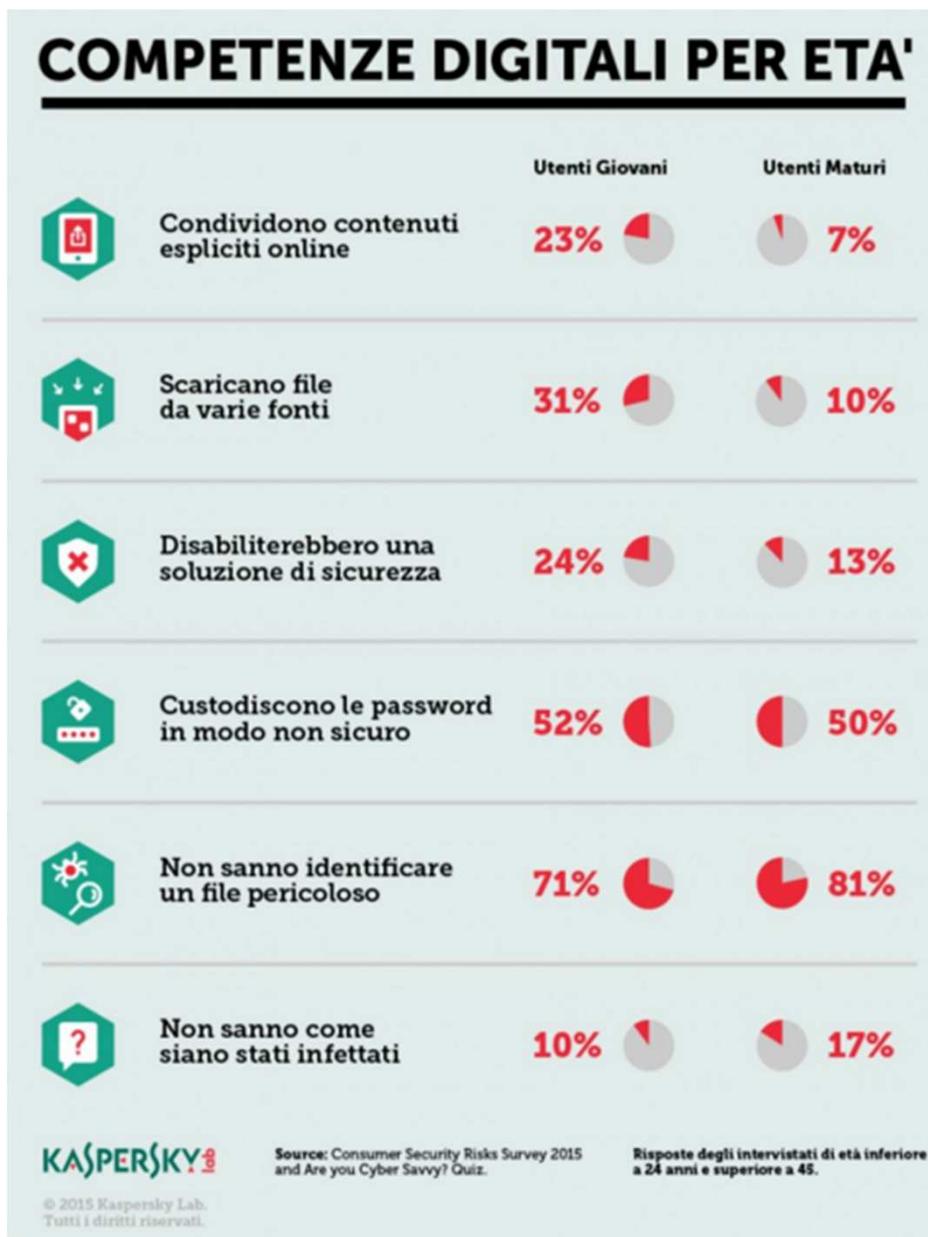
ESTRATTO DA:

<http://www.bitmat.it/blog/news/51484/giovani-vs-senior-chi-si-protegge-meglio-online>

Minacce comportamentali: competenze digitali per età

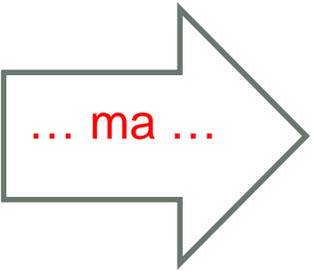
ESTRATTO DA:

<http://www.bitmat.it/blog/news/51484/giovani-vs-senior-chi-si-protolge-me-glio-online>



Responsabilità: spesso non percepita

« ... Le minacce esposte potrebbero facilmente essere trascurate in quanto le azioni da porre in essere per evitarle potrebbero richiedere sforzi rilevanti; taluni potrebbero ritenere tali **sforzi inutili o non motivati** da rischi su cui potenzialmente ci si potrebbe imbattere e verso i quali potrebbero non essere avvertite particolari forme di responsabilità... »



... ma ...

le norme riconducibili al Codice della Privacy, obbligano automaticamente i Titolari del Trattamento ad attivare le necessarie soluzioni organizzative, comportamentali e tecnologiche.

ATTENZIONE: delegare non esime necessariamente dalle responsabilità

Conclusioni

Anche nella formazione e la didattica per incrementare la cyber security occorre un incremento dell'**assunzione di consapevolezza** da parte degli attori coinvolti:

- ❑ **non è un tema nuovo**, anche nei settori della società che più rapidamente avevano accettato la sfida dell'innovazione digitale si era rilevata la stessa problematica
 - ma il settore della didattica e della formazione sembra essere rimasto un passo indietro
- ❑ ma l'esperienza maturata in altri settori può essere più facilmente ereditata da quanti sono giunti dopo, **oggi sono già disponibili**:
 - soluzioni tecnologiche
 - modelli organizzativi
 - quadri regolatori



Bibliografia

[Bach, 2015] Bach O., Mobile Malware Threats in 2015: Fraudsters Are Still Two Steps Ahead, IBM Security Intelligence (13 luglio 2015), 2015.

[Baldoni e De Nicola, 2015] Baldoni R., De Nicola R., Il Futuro della Cyber Security in Italia, Consorzio Interuniversitario Nazionale per l'Informatica, Laboratorio Nazionale di Cyber Security, 2015.

[Chiapasco e Cario, 2014] Chiapasco E., Cario M., CYBERBULLISMO dalle prime definizioni ai dati più recenti, Centro Studi Psicologia e Nuove Tecnologie, 2014.

[Clusit, 2016] Clusit, Rapporto Clusit 2016 sulla Sicurezza ICT in Italia, 2016.

[Commissione europea, 2001] Commissione europea, Piano d'azione eLearning. Pensare all'istruzione di domani, Bruxelles, 28.3.2001, COM(2001)172 definitivo, 2001.

[CSU, 2016] Colorado State University, Learning@CSU Guide: Core Rules of Netiquette, 2016.

[Di Maggio, 2014] Di Maggio C., Il Piano Nazionale Scuola Digitale – verso la Scuol@ 2.0, in Sfide e opportunità dell'Agenda digitale, Università di Bari e Stati Generali dell'Innovazione, 2014.

[HP, 2013] Hewlett-Packard Development Company, Reducing security risks from open source software, 4AA0-8061ENW, October 2013, Rev. 1, 2013.

[ENISA, 2016] European Union Agency For Network And Information Security, ENISA Threat Landscape 2015, 2016.

Bibliografia

[Massimini, 2006] Massimini M., Polytecna S.a.s., Il responsabile del trattamento, <http://www.privacy.it/massimini01.html>, 2006.

[Muzzi, 2013] Muzzi C., Big Data: limitazioni e opportunità geopolitiche e geoeconomiche, Atti del Congresso Nazionale AICA 2013, Salerno, 2013, 714-723.

[SOPHOS, 2013] Sophos in collaborazione con il Center for Internet Security, Threatsaurus - Le minacce a cui sono esposti computer e dati, dalla A alla Z, 1090-10DD.it.simple, 2013.

[WENATCHEE, 2010] Wenatchee Valley College, Netiquette guidelines for online students-Distance Learning Program, 2010.