AICA

UNIVERSITÀ DEGLI STUDI DI UDINE
hic sunt futura

DIDATTICA INFORMATICA 2016

30ª EDIZIONE DEL CONVEGNO

La Cyber Security come competenza per l'innovazione

«Cyber Security nella formazione e nella didattica»

Carlo Muzzì
muzzi@acm.org

UNIVERSITÀ DEGLI STUDI DI UDINE

SCUOLA SUPERIORE

19 aprile 2016
http://didamatica2016.uniud.it

Abstract

Cyber Security nella formazione e nella didattica

Carlo Muzzì
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 ciberspazio 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

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-ˌkyůr-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

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.

conseguenza

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

ESTRATTO DA: http://fedscoop.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.

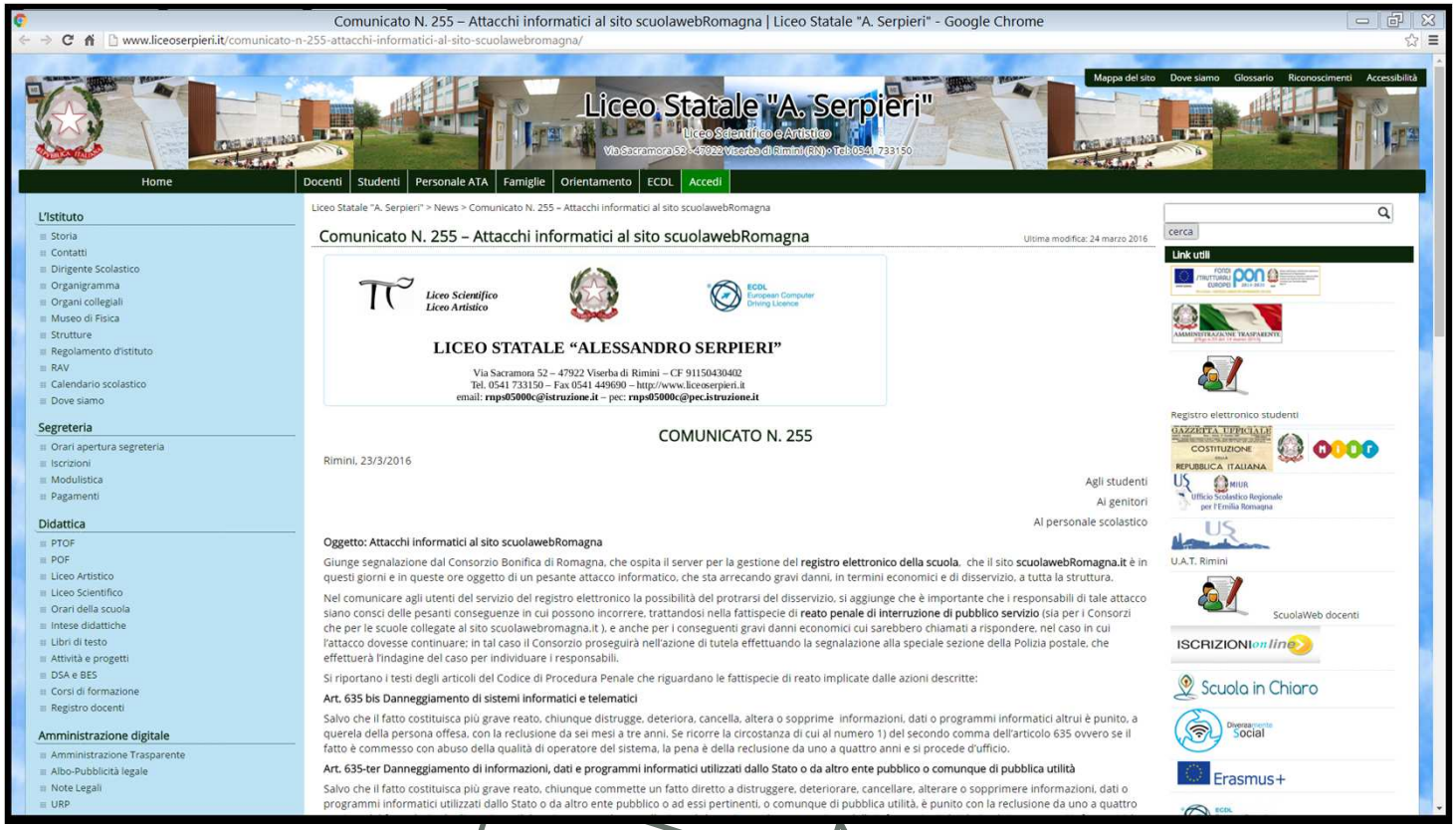
Ringraziando per l'attenzione si porgono distinti saluti.

Il Dirigente Scolastico

Blocco accessi al registro elettronico!

ESTRATTO DA: dalla cache di Google di un sito un Istituto Comprensivo ****

Un altro caso nella scuola italiana

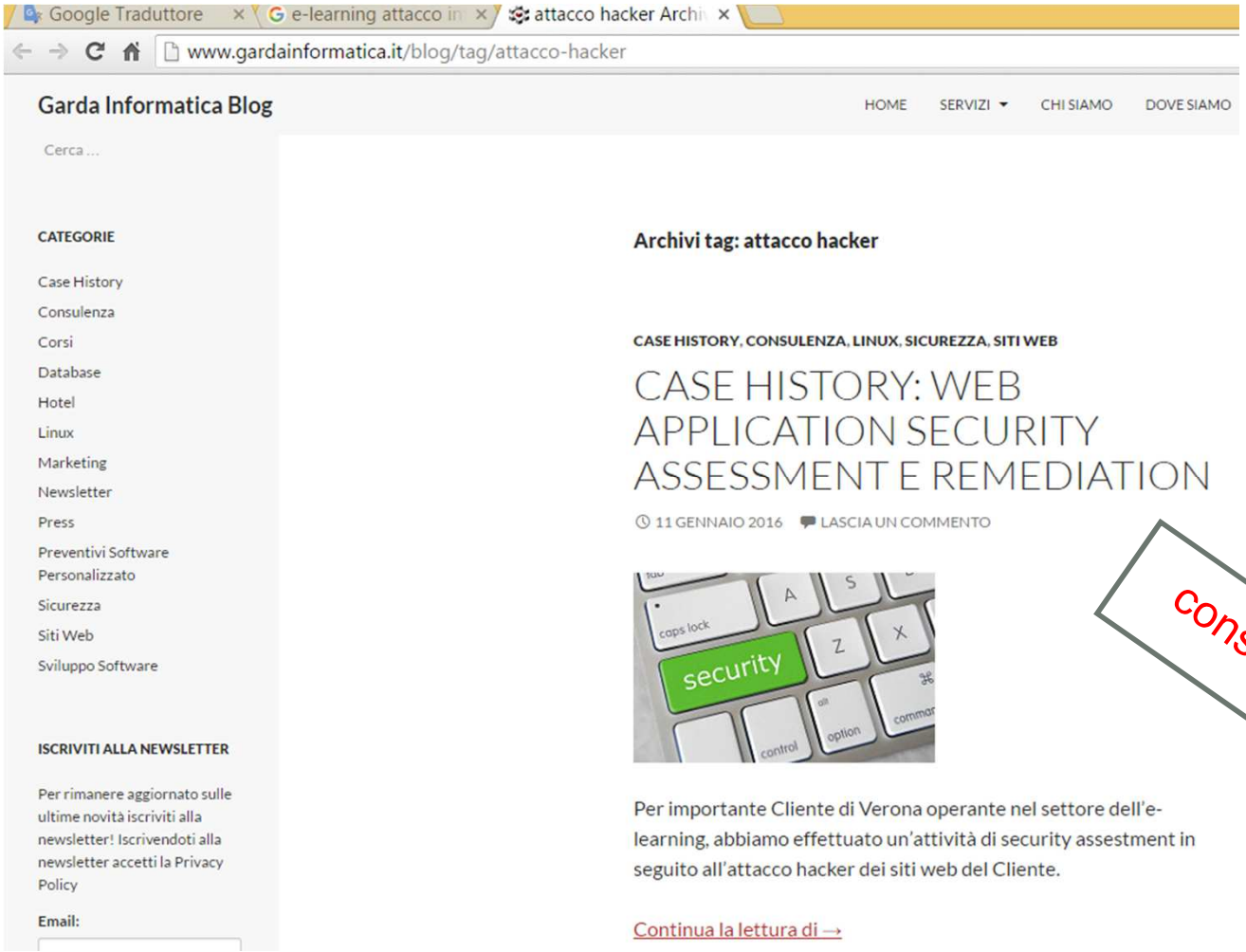


conseguenza

Ancora un blocco agli accessi del registro elettronico!

ESTRATTO DA: http://www.liceoserpieri.it/comunicato-n-255-attacchi-informatici-al-sito-scuolawebromagna/

Un caso nell' e-learning italiano



conseguenza

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 | NuovaEuropa | Latina | Brasil | English | Realestate

ANSA.it 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
Stampa
Scrivi alla redazione

Pubblicità 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.

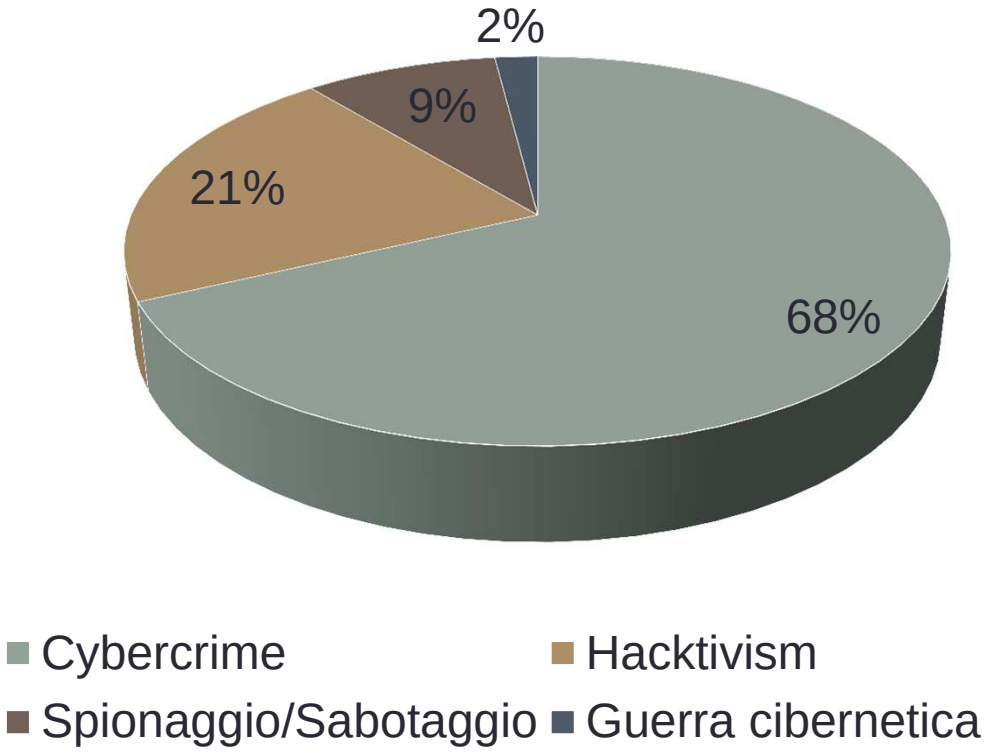
conseguenza

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



a) Tipologia e distribuzione degli attacchi nel 2015

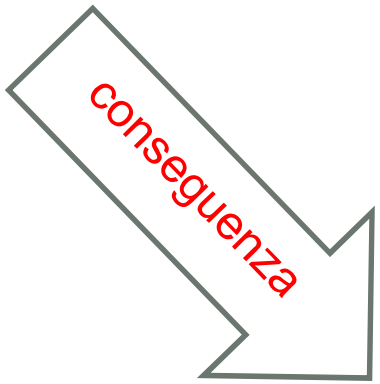
Dettaglio sul Cybercrime	2011	2012	2013	2014	2015	2012 su 2011	2013 su 2012	2014 su 2013	2015 su 2014	Trend 2015
	170	633	609	526	684	272,35%	-3,79%	-13,63%	30,04%	in aumento

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 (programme 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

Nascita dell'applicazione web

applicazione con successo

applicazione senza successo

ciclo di vita residuale

applicazione zombie ?

ma il successo il successo di un'applicazione commerciale genera anche profitti …

… e quindi investimenti sulla sicurezza sono anche possibili

ma se un applicazione è molto usata è più a rischio

paradosso

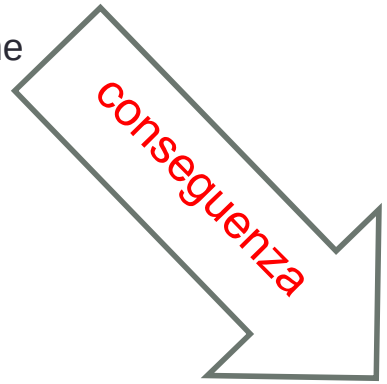
Ma nel caso in un'applicazione non commerciale i maggiori fondi per la security vi sarebbero ?

Ove mancassero il successo sarebbe stato addirittura controproducente !

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



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 (programme 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

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

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.

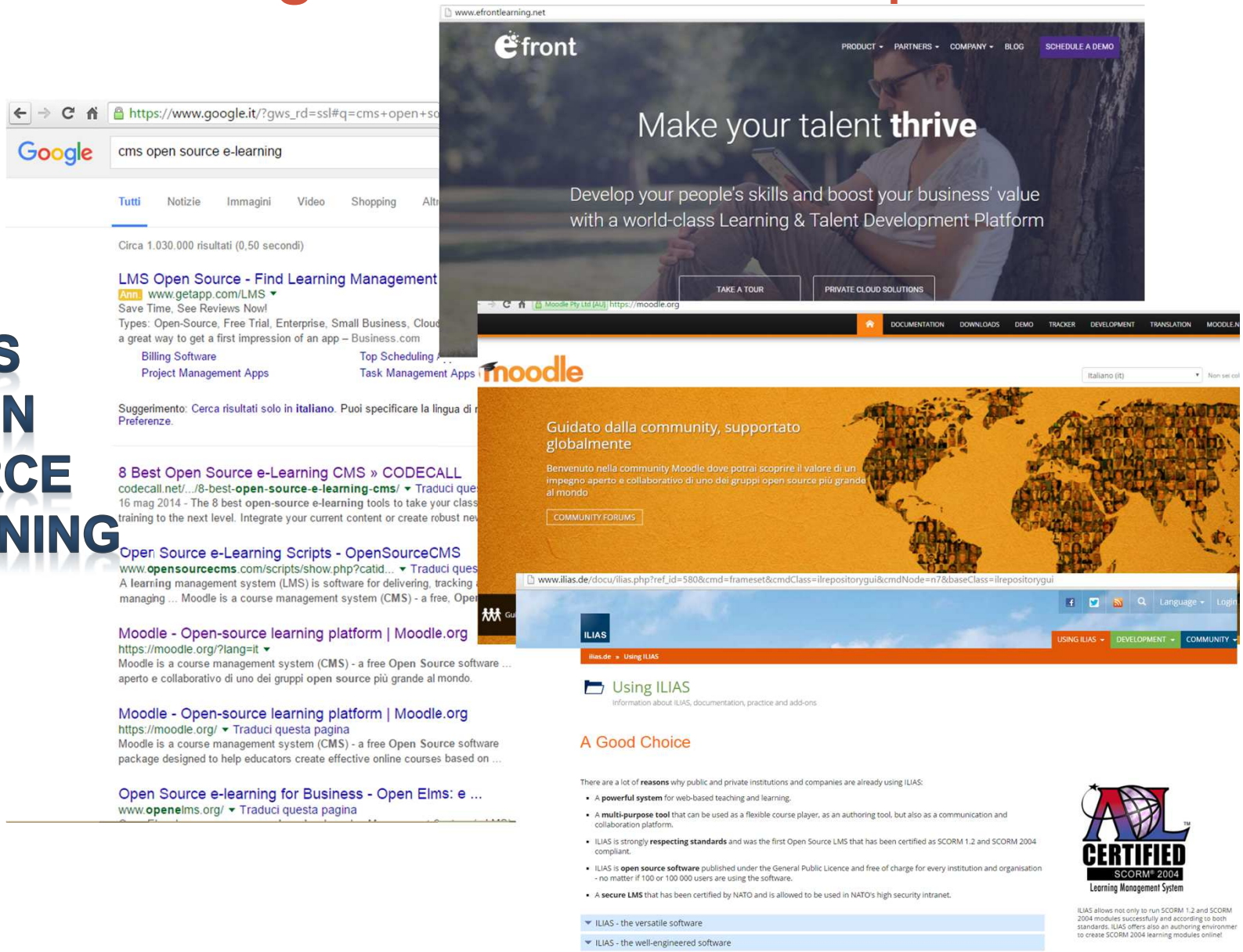
FONTE: Di Maggio C., Il Piano Nazionale Scuola Digitale – verso la Scuol@ 2.0, 2014

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...»*

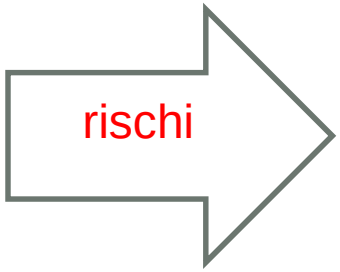
Minacce tecnologiche: le soluzioni «pronte all'uso»

CMS OPEN SOURCE E-LEARNING



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 d**i controllo dello strumento tecnologico** da parte dei docenti → i rischi dei discenti «che ne sanno di più»

Minacce comportamentali: differenze generazionali

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

BitMat
Tv • Dossier on demand
Cerca...
NEL SITO
NEL NETWORK
> NEWS > TECNOLOGIE > INTERNET > MERCATI > APP > DEVICE > RUBRICHE >

RED 2016
Riviera Engineering Days
ingegneria del turismo
agenda digitale
big data
efficenza energetica
smartgrid
creazione d'impresa
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

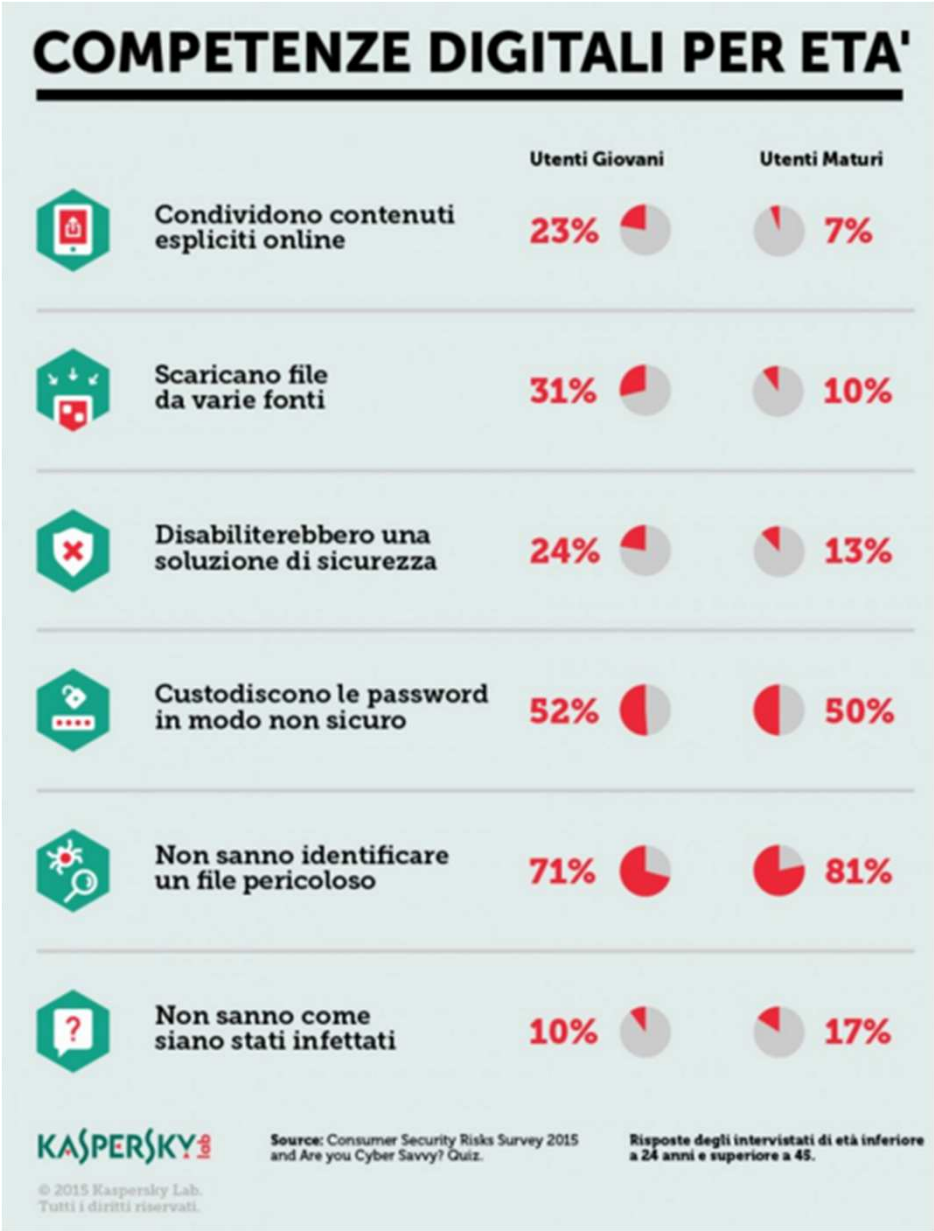
Kaspersky, sicurezza

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.

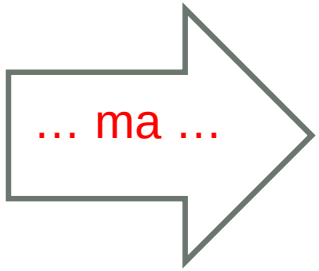
Minacce comportamentali: competenze digitali per età

ESTRATTO DA:
http://www.bitmat.it/blog/news/51484/giovani-vs-senior-chi-si-protegge-meglio-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…»*



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.

[Muzzì, 2013] Muzzì 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.