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.*

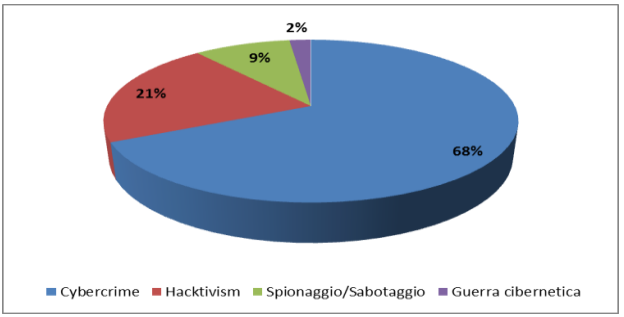
1. Introduzione

Questo millennio è nato nella dimensione digitale, non solo le attività professionali ma anche la socialità di ogni individuo si esprime in uno spazio virtuale divenuto generalmente pervasivo; naturalmente anche la didattica e la formazione hanno accettato la sfida lanciata da questa nuova dimensione, che è divenuta un volano per l'innovazione dei processi formativi. Ma l'esistenza digitale porta con sé anche quelle nuove problematiche identificate col termine cyber security (sicurezza cibernetica o sicurezza digitale); purtroppo le potenziali minacce che ne conseguono non sono sempre adeguatamente percepite e quindi nemmeno gestite: questo studio discuterà di svariati scenari di rischio ritenuti tipici nel contesto formativo.

2. Il ruolo della rete

Una trattazione sulla Cyber Security non può non considerare il significativo ruolo che la rete ha assunto anche nel mondo della formazione e della didattica; del resto la stessa Unione Europea ha identificato l'e-learning come "l'utilizzo delle nuove tecnologie multimediali e di Internet per migliorare la qualità dell'apprendimento agevolando l'accesso a risorse e servizi nonché gli scambi e la collaborazione a distanza" [Commissione europea, 2001]. Ma naturalmente internet non è solo il luogo delle opportunità; purtroppo le possibilità di relazione e interazione offerte dallo strumento sono anche sfruttate per finalità negative o addirittura illecite: è quindi necessario che i temi della cyber security siano adeguatamente considerati anche da chi si occupa di formazione o didattica.

Questa esigenza non sembra scemare col tempo; in effetti il rapporto Clusit 2016 sulla sicurezza ICT [Clusit, 2016] evidenzia come il 68% dei 1.052 gravi attacchi di pubblico dominio classificati in Italia nel 2015 abbiano proprio riguardato gli attacchi cybercrime (vedi Fig. 1.a) ed inoltre l'analisi comparata sul periodo 2011-2015 (vedi Fig. 1.b) denota anche che per tali attacchi, dopo 2 anni di riduzione, si sia nuovamente riscontrato un incremento del 30,04%: con un trend atteso in aumento.



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

Fig. 1 – Rapporto Clusit 2016 sulla Sicurezza ICT in Italia

Questi dati evidenziano anche ai non esperti di cyber security che l'evoluzione delle misure di sicurezza che vengono adottate in modo sempre più standard nei sistemi ICT non sembrano poter costituire la soluzione sufficiente a trasformare la rete in quell'area asettica e priva di rischi che molti desidererebbero. Azioni specifiche e attenzioni continue sono quindi necessarie per poter combattere quelle nuove minacce che nascono ogni giorno come risvolto negativo del progressivo aumento di dipendenza dal cyberspace [Baldoni e De Nicola, 2015].

Nel seguito verranno sinteticamente trattate le minacce ritenute più significative per quella particolare area del cyberspazio che coinvolge quanti si occupano di formazione e didattica.

2.1 Minacce tecnologiche

Lo spazio cibernetico è tale proprio grazie alle possibilità offerte dalla pervasività tecnologica che ci circonda; ne consegue che le minacce di tipo tecnologico siano le prime a dover essere considerate. Naturalmente il vasto

tema della sicurezza del web ha ricadute anche nelle applicazioni dedicate alla formazione e, più generalmente, alla didattica: su cui ricadano tutte le minacce tipiche delle piattaforme web. Se infatti si analizzano le molteplici **piattaforme di e-learning**, siano esse nazionali o internazionali, basate sul modello dei cloud generalisti o su soluzioni proprietarie, si rileva che nella generalità dei casi le stesse 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 (per sua natura dinamico e adattivo rispetto alle peculiarità di ogni discente), profilare il discente ed il progresso del suo apprendimento rispetto a quanto erogato, gestire le informazioni tecniche necessarie all'operatività dei siti dinamici;
– gestire il rapporto con l'utente sia attraverso gli strumenti più tradizionali (quali: e-mail, chat, tutorial) e sia tramite quelli più tipici del mondo dei social media e delle piattaforme di contenuti multimediali (ad esempio: Facebook e YouTube).

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

Fig. 2 –ENISA ETL 2015: Panorama delle minacce cibernetiche del 2015

Non è necessario approfondire oltre per comprendere come, dal punto di vista tecnologico, le piattaforme di e-learning non siano altro che finalizzazioni specifiche delle tradizionali piattaforme web e, di conseguenza, siano soggette alle stesse minacce che gravano su queste ultime. Il rapporto dell'*European Union Agency for Network and Information Security* sulle cyber-minacce per il 2015 [ENISA, 2016] permette immediatamente di cogliere il quadro totale dei rischi (vedi Fig. 2) e come molti di queste abbiano un potenziale impatto nel contesto in esame.

Avendo in comune le stesse problematiche dovremmo attenderci che possano condividerne anche le soluzioni correttive e preventive o le medesime misure contenitive dei danni. Purtroppo questo è vero solo in linea teorica, la realtà può essere diversa perché nel mondo della formazione il contesto in cui è

attivo l'operatore formatore può causare effetti imprevedibili dal punto di vista della cyber security.

Consideriamo, ad esempio, il caso una piattaforma *e-learning* di tipo commerciale: probabilmente disporrà di una infrastruttura tecnologica gestita in modo professionale e verosimilmente disporrà delle risorse economiche ed umane sufficienti per gestire queste minacce a livelli non dissimili da una qualsiasi altra applicazioni web commerciale. Ma le piattaforme gestite da contesti più istituzionali, ad esempio ministeri, università, scuole superiori o altri organismi pubblici, avrebbero le stesse risorse? È evidente come in questo caso lo scenario si complichi sensibilmente: se una soluzione commerciale ha successo significa che cresce; nel contesto di internet questo però significa che cresceranno anche i rischi e di conseguenza l'esigenza di ampliare le contromisure; saranno quindi necessarie più risorse ma è verosimile che queste potrebbero essere disponibili perché il successo in un'attività commerciale genera profitti che possono essere reinvestiti anche in sicurezza. In un contesto pubblico ciò non è necessariamente vero: il rapporto risorse-risultati è legato in modo molto meno stringente, perché un'istituzione riceve (quando li riceve) dei fondi che non sono necessariamente commisurati ai risultati che raggiunge (o con tempistiche congruenti). Ne discende il paradosso che, per tale contesto, il successo di una piattaforma e-learning potrebbe addirittura essere controproducente dal punto di vista della cyber security.

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

Fig. 3 –ENISA ETL 2015: Minacce emergenti e trend nel Mobile Computing

Col *M-learning* si identifica quell'apprendimento che avviene attraverso l'ausilio di dispositivi mobili come PDA, smartphone, netbook, riproduttori audio e video digitali e tutta una serie di altri strumenti trasportabili che permettono di produrre un'offerta formativa fruibile in ogni momento della vita quotidiana. Quando questa formazione avviene con strumenti connessi alla rete, il discente utilizza tablet e smartphone connesse a quelle che possiamo identificare come **piattaforme M-learning**.

Dal punto di vista dei rischi del cyberspazio queste piattaforme ereditano le minacce tecnologiche dell'e-learning aggiungendovi quelle tematiche di security tipiche del mondo mobile; la consultazione del rapporto [ENISA, 2016] è utile

anche nel settore del mobile computing per analizzare le minacce emergenti e le loro tendenze (vedi Fig. 3).

È noto che in tale mondo le contromisure di sicurezza, anche quando esistono, sono scarsamente utilizzate in quanto gli utilizzatori di tablet o smartphone hanno una naturale tendenza ad utilizzarli come fossero appendici tecnologiche del proprio corpo, delle estensioni artificiali della propria esistenza: questa visione personalistica dello strumento (in fin dei conti simile a quella che ha portato alla primitiva definizione di personal computer) induce nell'utilizzatore un livello di fiducia estremamente elevato che ne impedisce di percepire le potenziali minacce. È interessante notare come anche coloro che sono attenti a proteggere le proprie attività in rete quando utilizzano un computer tradizionale -utilizzando password, antivirus, e buone prassi- non adottano le medesime cautele quando usano tablet o smartphone ritenendole superflue. Invece i cybercriminali hanno ben compreso come sfruttare queste lacune comportamentali; monitoraggi effettuati [Bach, 2015] nel primo semestre del 2015 hanno evidenziato come il tasso di infezione per malware sui dispositivi mobile sia in effetti lo stesso dei PC.

L'importanza del M-learning nel nostro contesto nazionale è anche legato alle proposte –come quella di [Di Maggio, 2014]- avanzate nella scuola italiana di utilizzare questi strumenti, di cui ormai buona parte degli studenti e docenti italiani sono in possesso e portano sempre con se (BYOD, Bring Your Own Device), per effettuare quella formazione didattica in rete che non risulta possibile con le dotazioni tecnologiche delle scuole che, purtroppo, spesso mancano o sono insufficienti.

Naturalmente questo approccio ha un riflesso di sicurezza informatica negativo addizionale: 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.

2.2 Il rischio delle soluzioni "pronte all'uso"

Anche nel campo della formazione a distanza è avvertita l'esigenza di comprimere i costi e i tempi di realizzazione delle soluzioni applicative informatiche necessarie ad erogare i contenuti formativi: la scelta di rivolgersi a soluzioni **"pronte all'uso"** costituisce quindi un bacino di riferimento naturale.

In effetti la rete rende disponibili un'innumerevole serie di strumenti che possono essere utilizzati, in modo singolo o in aggregazione, per giungere alla realizzazione della soluzione attesa (del resto è sufficiente ricordare come una generica piattaforma CMS -content management system o sistema di gestione dei contenuti- possa costituire l'infrastruttura di base da cui partire per erogare contenuti informativi di vario genere). Ma quando a queste soluzioni ci si rivolge spinti da necessità economiche, ossia perché si dispongono di budget limitati

per gli investimenti informatici, ecco che i rischi di sicurezza aumentano: è purtroppo il settore dell'educazione è cronicamente afflitto dalla scarsa disponibilità di risorse!

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 [HP, 2013]; per gestirli occorre anche reinvestire una parte di quelle risorse risparmiate con l'utilizzo delle soluzioni aperte.

È noto come l'open source sia spesso consigliato nel mondo della cyber security perché consente di poter eseguire controlli sul codice sorgente per accertare che il software ottenuto svolga solo e soltanto le elaborazioni dichiarate: ma l'esecuzione di una tale attività di controllo avrà un costo. È anche noto come talvolta il processo di sviluppo delle soluzioni informatiche preveda di utilizzare un substrato di componenti applicative ed infrastrutturali di utilizzo libero su cui innestare le successive attività di adattamento: tale processo non garantisce necessariamente che l'utilizzo di componenti di base con un buon livello di sicurezza conduca a risultati finali con analogo livello, ma destinando le opportune risorse questi risultati saranno verosimilmente raggiunti.

Sulla base di queste considerazioni emerge che in una soluzione di tipo commerciale il fornitore della stessa ha obblighi, non solo contrattuali ma anche legali, che lo spingeranno a realizzare un buon prodotto (o a prestare un valido servizio) che tenga anche in conto degli aspetti di sicurezza sui quali potrebbe comunque essere chiamato a rispondere; mentre nelle soluzioni aperte, come in quelle "pronte all'suo", la committenza ha maggiori gradi di scelta: potrebbe - ed è auspicabile lo faccia- dedicare (o commissionare a terzi) sforzi e risorse anche all'area della sicurezza cibernetica oppure potrebbe decidere di massimizzare i risparmi ottenuti evitando del tutto questi costi che, anche per inconsapevolezza sulle minacce, potrebbe ritenere superflui. È comunque da attendersi che questo spazio di discrezionalità di cui oggi la committenza dispone, venga comunque ridotto con l'entrata in vigore del nuovo regolamento europeo per la protezione dei dati personali, che imporrà maggiori obblighi sulla produzione del software e tra l'altro in un quadro giuridico più uniforme a livello continentale [Muzzì, 2013].

2.3 Minacce comportamentali

I comportamenti degli individui sono ormai generalmente accettati come fattori di rischio significativo per ogni attività umana che utilizza applicazioni informatiche; nel contesto della nostra trattazione non ci focalizzeremo sulle minacce (e relative contromisure) che colpiscono il cyberspazio in generale [SOPHOS, 2013], quanto alcuni rischi comportamentali ritenuti più tipici nella didattica e nella formazione.

Il primo di questi rischi è riconducibile alla sfera della **protezione delle credenziali** di utilizzo dei sistemi. Non ci si riferisce tanto alla gestione oculata

dei propri codici identificativi e di autenticazione, aspetto essenziale ma banale, quanto piuttosto alla tendenza a condividere tra gruppi di individui (classi virtuali, comunità di discenti, ecc.) utenze e password di accesso a servizi informatici originariamente "pensati" per utilizzi individuali o personali. Se è naturale scegliere il cyberspazio quando si ha l'esigenza di un'area pubblica in cui condividere contenuti multimediali (documenti, file, immagini, ecc.), è invece deprecabile, per tutti i potenziali rischi che questa decisione comporta, creare un utente fittizio (magari legato ad una casella di posta o ad un'area di storage) per condividerne le credenziali tra tutti i membri: purtroppo è però usuale rilevare questi comportamenti scorretti anche quando questi sarebbero inutili, come nel cloud dove esistono già ecosistemi digitali in grado di gestire condivisioni controllate e correlate tra profili di singoli individui.

Ma il cloud è anche il luogo dove la **riservatezza dei contenuti** o la **violazione dei diritti di terzi** assumono una dimensione di rischio legale sempre più elevato. Proteggersi da questi rischi implica la definizione di un quadro regolatorio delle attività e l'adozione di una consapevole strategia di gestione delle stesse; per realizzarla occorre: definire il perimetro del quadro giuridico di riferimento, proceduralizzare le attività, implementare i mezzi tecnici per sostenerle e disporre di un livello di controllo o supervisione. La complessità gestionale dei temi da affrontare è uno degli elementi di rischio più significativo, basti pensare che molte piattaforme di contenuti multimediali pubblicano policy per il governo dei contenuti: ma quanti le conoscono o le applicano? Queste soluzioni sono auspicabili anche nel settore della formazione a distanza ed in effetti diversi organismi pubblicano netquette per gli studenti online [WENATCHEE, 2010] o per gli studenti in genere [CSU, 2016]: è una strada che occorrerebbe percorre a prescindere.

Un ulteriore rischio è naturalmente connesso al fenomeno del **cyberbullismo** [Chiapasco e Cario, 2014], noto anche come ciberbullismo o bullismo online, che non deve assolutamente essere trascurato neanche all'interno della formazione on-line. Il rischio che comportamenti sconvenienti possano screditare la personalità di un individuo, spingendolo verso azioni talvolta imprevedibili, potrebbe essere addirittura enfatizzato nel settore della formazione a distanza: soprattutto quando questa avvenisse all'interno di gruppi chiusi e legati da una comunanza di fini intellettuali.

Infine, una considerazione più generale riguardante le attività delle scuole secondarie di I e II grado. In questi istituti il rapporto gerarchico docente-studente, basato sul paradigma del trasferimento di competenza dal soggetto con autorità verso i propri allievi, può essere minato e talvolta ribaltato quando la formazione avviene con strumenti tecnologici. Il rischio di **perdita di autorità o di controllo dello strumento tecnologico** da parte del docente, rispetto a discenti che spesso "ne sanno più di lui", potrebbe condurre ad effetti inaspettati.

3. Responsabilità

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.

Tralasciando gli aspetti etici di una tale forma di pilatismo è opportuno rammentare come, già solo nel panorama italiano ed europeo, vi siano responsabilità varie.

Le norme riconducibili al Codice della Privacy (d.lg. 30 giugno 2003 n. 196, che ha attuato nell'ordinamento giuridico italiano la direttiva comunitaria 95/46/CE) obbligano a porre in essere le soluzioni organizzative, comportamentali e tecnologiche in capo ai cosiddetti Titolari del Trattamento: ossia ai soggetti che effettuano la formazione e la didattica. Questi sono coloro che innescano il processo formativo e sono quindi i titolari dei dati dei soggetti coi quali interagiscono: sono pertanto automaticamente responsabili dei trattamenti effettuati sui dati stessi. La scelta di gestire con altri soggetti, come gli incaricati o responsabili del trattamento, non libera da responsabilità se tali incarichi non sono stati opportunamente formalizzati, gestiti, ma soprattutto controllati [Massimini, 2006]. Ad esempio, anche nel caso di outsourcing di talune attività, i soggetti esterni incaricati divengono dei responsabili del trattamento verso i quali però permangono gli obblighi di verifica del buon operare da parte del Titolare: delegare non esime dalle responsabilità.

3. Conclusioni

Le minacce discusse in questo articolo hanno evidenziato svariati scenari di rischio connessi alle minacce dell'era digitale per la formazione e la didattica; anche in questo contesto è emerso come uno degli elementi essenziali per poterli gestire è l'assunzione di consapevolezza, da parte degli attori coinvolti, sulle tematiche della cyber security: consapevolezza, spesso, non avvertita.

Non si tratta di 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 mentre questi settori hanno superato questa fase, l'ambito della didattica e della formazione, così variegato e multiforme, sembra essere rimasto un passo indietro.

Questa situazione non è però solo foriera di considerazioni negative, l'esperienza maturata in altri settori può essere più facilmente ereditata da quanti sono giunti dopo: le soluzioni tecnologiche, i modelli organizzativi, i quadri regolatori già disponibili permetteranno di gestire questi temi anche a costi inferiori da quelli sostenuti da quanti li hanno già affrontati in passato.

Naturalmente occorrerà accettare la sfida, ignorarla sarà inutile: l'esigenza di confrontarsi con la generazione digitale che popola le nostre scuole e la continua interazione in rete dell'esistenza globalizzata che ormai tutti viviamo, ci obbligheranno comunque ad affrontarla.

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.

[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.