TEMA

Sicurezza informatica: quello che le scuole devono sapere

Francesca Palareti

Università degli Studi di Firenze

francesca.palareti@unifi.it

Il webinar, che analizzeremo nelle sue linee sostanziali, è stato organizzato da Formez PA – Centro servizi, assistenza, studi e formazione per l'ammodernamento delle P.A., organo promosso dal Dipartimento della Funzione Pubblica – ed è rivolto a DS/DSGA/Assistenti amministrativi degli istituti scolastici[1].

Figura 1 – Webinar (http://eventipa.formez.it/node/39374)

[1] Il webinar è liberamente accessibile sul sito Formez PA tramite piattaforma di video-conferenza a partire dalla pagina http://eventipa.formez.it/node/39374.

Svoltosi a febbraio 2015, il seminario si inserisce nell'ambito del progetto formativo "Semplificazione e nuovo CAD – Codice dell'Amministrazione Digitale"[2], che rientra nella programmazione comunitaria volta a potenziare la capacità istituzionale e la *governance* interna degli istituti scolastici e delle strutture del comparto istruzione. Affronta in modo efficace e da diverse prospettive di analisi le problematiche legali e le criticità legate alla digitalizzazione dei procedimenti amministrativi e la conseguente necessità di garantirne la sicurezza, con l'obiettivo di fornire indicazioni utili alla progettazione di sistemi a norma di legge.

Il primo intervento, curato da un legale, ripercorre la normativa di riferimento e suggerisce le misure da implementare nelle scuole per la sicurezza dei sistemi informatici. Il relatore, Avv. **Francesco Micozzi**, richiama inizialmente le disposizioni previste dal CAD (D. Lgs. 82/2005), il quale all'art. 40 prevede che i documenti creati dalla P.A. nascano – e di conseguenza vengano gestiti, trasmessi e conservati – in formato digitale. La P.A. esercita ormai la sua attività in una nuova dimensione che prescinde dall'analogico, di conseguenza non è più ammissibile ignorare le regole della sicurezza, da intendersi come processo dinamico in continuo divenire capace di adattarsi alle emergenze contingenti. È necessario, quindi, adottare preventivamente tutte le cautele possibili per evitare che venga lesa l'integrità dei dati, con un'accurata analisi delle minacce e strategie di riduzione del rischio.

Ogni sistema informatico è costituito da hardware, software e wetware, termine con il quale si identifica il fattore umano, spesso all'origine di danni generati da un'errata interazione con gli strumenti informatici. Un fattore di rischio sempre più attuale, infatti, è rappresentato dai frequenti attacchi con sistemi di *Social Engineering* basati proprio sull'elemento umano debole che attua comportamenti incauti, in considerazione dei quali è sempre più indispensabile investire nella formazione per l'acquisizione di competenze tecniche e la conoscenza della normativa vigente.

Le misure di sicurezza a cui attenersi sono definite dal legislatore nel D. Lgs. 196/2003, meglio conosciuto come Codice della Privacy. Esso prevede **misure idonee** (art. 31 "Obblighi di sicurezza") che devono essere adottate nell'immediatezza dei fatti – misure atte ad evitare la perdita anche accidentale di dati, l'accesso non autorizzato e il trattamento dei dati non consentito o non conforme alle finalità della raccolta – e **misure minime** (art. 33) di protezione dei dati personali, la cui inosservanza comporta responsabilità civile e penale. Queste ultime misure prevedono principalmente le seguenti pratiche:

- sistemi di autenticazione informatica tramite utilizzo di credenziali (username e password, chiavi di almeno 8 caratteri che non devono ricondurre in alcun modo all'interessato, da modificare almeno ogni sei mesi; nel caso di dati sensibili e/o giudiziari almeno ogni tre mesi), di altri dispositivi (tesserino identificativo, badge, chiave hw) o di una caratteristica biometrica (DNA, sistema di impronte digitali/vocali, stile grafia, scansione retinica);

[2] Il progetto ha previsto attività in aula e a distanza, proponendo un ciclo di webinar approfondimento su tematiche strategiche a cura di esperti e testimoni di istituti scolastici che hanno maturato esperienze significative in materia.

- sistemi di autorizzazione, che consentono di differenziare i privilegi di accesso allo stesso sistema informatico da parte di più soggetti tramite profilazione;
- soluzioni anti-intrusione e anti-virus da aggiornare con cadenza semestrale (per il software, invece, è raccomandato un aggiornamento con cadenza annuale);
- backup settimanale dei dati (sebbene sia consigliabile effettuarlo quotidianamente);
- utilizzo di supporti removibili, nonché adozione di sistemi di *wiping*[3] sui supporti removibili inutilizzati e sistemi di *data recovery* nei 7 giorni per consentire il ripristino dei dati. Le P.A., a tale proposito, sono tenute a definire un piano di continuità operativa e a dotarsi di un piano di *disaster recovery* per un rapido ed efficace recupero delle informazioni.

Il secondo intervento del webinar, tenuto dal DS dell'I.I.S.S. "Ettore Majorana" di Brindisi, **Salvatore Giuliano**, dal taglio più operativo, espone la capillare infrastruttura di rete del suo istituto e le misure di sicurezza adottate, soffermandosi sulle pratiche messe in atto al fine di evitare possibili manomissioni e perdite di dati.

Nella sua relazione Giuliano parte dalla constatazione che, essendo l'informazione un bene aziendale, ormai in gran parte custodita su supporti digitali, ogni organizzazione deve essere in grado di salvaguardare l'integrità dei propri archivi in un contesto in cui i rischi informatici causati da violazione dei sistemi di sicurezza sono in continua crescita.

La sicurezza deve riguardare in prima analisi il sistema operativo adottato – privilegiando sistemi *open* – ed i software, componenti fondamentali di ogni rete informatica, evitando la pratica molto diffusa di installare programmi privi di licenza, rischiando in tal modo di esporsi a reati oltre che a minacce di malware. Altra componente da monitorare è la comunicazione che dalla scuola raggiunge altri destinatari, che deve rispettare alcuni parametri di base per non incorrere nel rischio di eludere i criteri minimi previsti dalla normativa.

Il Dirigente scolastico, poi, avvalendosi della consulenza del responsabile di rete, passa ad analizzare le principali tecniche di attacco informatico – port scanning, sniffing, keylogging, DoS, backdoor, buffer overflow – e quelle di difesa – antivirus, antispyware, firewall, firma digitale, crittografia, backup, intrusion detection system – per poi illustrare la struttura di rete dell'Istituto Majorana.

[3] Tecnica informatica che consiste nella cancellazione sicura e definitiva dei dati tramite sovrascrittura dei file eseguita più volte al fine di renderli irrecuperabili.

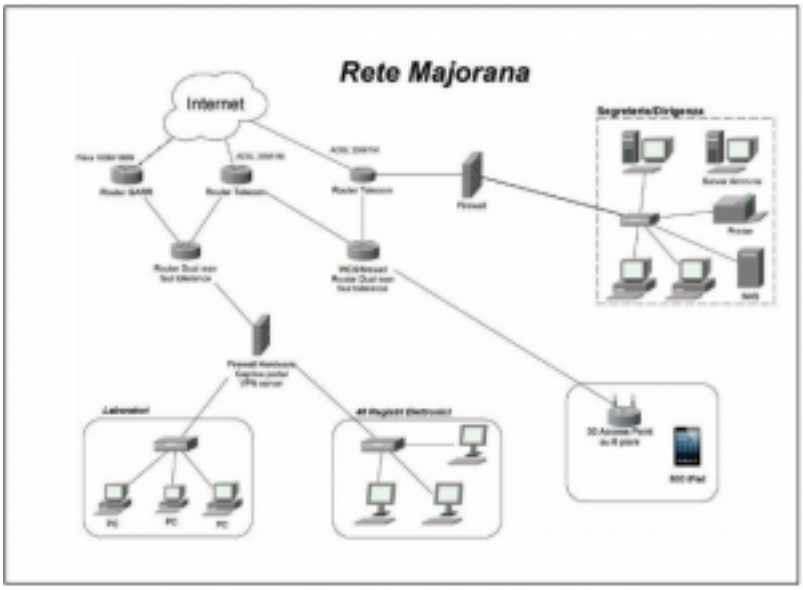

Figura 2 – Rete dell'I.I.S.S. "Ettore Majorana" di Brindisi.

Questa si avvale di tre router, che presidiano altrettante linee di navigazione, due ADSL ed una connessione in fibra ottica, di cui due linee attive ed una ADSL utilizzata come linea di emergenza in caso di malfunzionamento delle altre mediante router dotati di più ingressi wan. L'altra linea ADSL è ad uso esclusivo di segreteria e dirigenza per garantire una maggiore sicurezza dei dati, separandone il flusso da quello proveniente dai laboratori scolastici; all'interno di essa è stato installato un NAS[4] che effettua il backup giornaliero dei dati più importanti.

Un dispositivo WCS (Wireless Control System) controlla l'intera rete wireless attraverso 30 *Access Point* dislocati su 6 piani, garantendo l'accesso tramite autenticazione a 150 utenti simultanei. Ogni studente ha in dotazione un tablet, per un totale di 800 iPad utilizzati per la somministrazione di test e la distribuzione di contenuti didattici.

La terza linea, in fibra ottica, è fornita dal GARR, rete nazionale a banda ultralarga dedicata al mondo dell'istruzione e della ricerca, e gestisce i PC collocati nei laboratori ed i 40 registri elettronici, su cui è possibile caricare lezioni e materiali didattici.

L'installazione della fibra ottica all'interno dell'istituto è stata realizzata grazie all'adesione al progetto GARR Progress, convenzione rivolta alle scuole della Regione che garantisce una banda pari a 100 Mbps ed un altissimo livello di sicurezza informatica.

Avendo allestito una infrastruttura tecnologica così articolata e complessa, la scuola ha investito sulle necessarie competenze individuali, che prevedono in modo imprescindibile la conoscenza della normativa in relazione alla privacy nella PA, ed in

[4] Network Attached Storage (NAS) è un particolare dispositivo in grado di condividere il contenuto di uno o più dischi rigidi attraverso l'utilizzo di un'appropriata rete di computer. I NAS, però, non sono dei semplici "dischi di rete", ma si comportano come dei veri e propri server che permettono di condividere file, di effettuare copie di backup e di essere raggiunti da remoto.

particolare sulle competenze informatiche, al fine di attuare le migliori metodologie e strategie a tutela della riservatezza dei dati.

Gli obiettivi della sicurezza interna – quella maggiormente a rischio in considerazione del fatto che gli attacchi negli istituti scolastici provengano per lo più proprio dall'interno – riguardano la definizione di diritti e doveri degli utilizzatori, di regole e provvedimenti in caso di violazione delle stesse riguardanti l'utilizzo di dispositivi (PC, tablet), rete e posta elettronica e l'individuazione di un responsabile tecnico.

Tra le misure adottate per limitare un utilizzo non autorizzato della rete l'istituto ha previsto il rilascio di password a tempo e la disattivazione di tutte le user/pw alle ore 20.00, misura cautelare presa dopo aver riscontrato un anomalo traffico notturno[5].

Le criticità emerse hanno riguardato essenzialmente la realizzazione del nuovo cablaggio in funzione dei bisogni ed in particolare la necessità di incrementare il numero di utenze simultanee, nonché le nuove procedure di accesso per tutto il personale scolastico, con le diverse profilazioni previste nella pianificazione del nuovo sistema di autorizzazione.

In conclusione, alla luce del quadro delineato dal webinar, sarebbe auspicabile che ogni istituto scolastico si dotasse di una propria *policy* in materia di sicurezza contenente obiettivi e vincoli relativi all'utilizzo del sistema informatico, specificando diritti, risorse e modalità di accesso. Tale documento dovrebbe rappresentare il cardine delle linee guida, che traducono la politica di sicurezza in azioni e controlli. Definire e formalizzare le procedure significa favorire un uso consapevole degli strumenti informatici e promuovere un'educazione digitale al passo con l'innovazione tecnologica, al fine di arginare la vulnerabilità del sistema e tutelare l'organizzazione in presenza di reati e frodi.

La sicurezza va, quindi, intesa come parte integrante dei processi aziendali e costituisce una variabile critica trasversale a tutte le attività, che coinvolge tecnologia, organizzazione e logistica.

[5] L'intero traffico di rete di ogni istituto scolastico aderente al progetto GARR è pubblicato sul sito GARR, che garantisce anche un servizio statistico sugli accessi.