MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
Liceo Ginnasio Statale "Ennio Quirino Visconti"
con sezione Cambridge International School
Piazza del Collegio Romano, 4 - 00186 ROMA - Distretto 9 - C.F. 80240330581
Centralino tel 06 121124325/fax 06-67663882
rmpc080007@istruzione.it – rmpc080007@pec.istruzione.it
www.liceoeqvisconti.it

prot. n. 16128 01
Roma, 20 novembre 2014

FIREWALL E WEB FILTERING
IN ESSERE PRESSO IL LICEO VISCONTI

Premessa:
Informazione sui Reati e violazioni della legge connessi con l'uso della Rete informatica

Oltre alle regole di buona educazione che governano le relazioni interpersonali, appare opportuno ricordare che ci sono comportamenti, talvolta apparentemente innocui, che possono portare gli autori a commettere veri e propri reati e, di conseguenza, a subire procedimenti penali dalle conseguenze anche gravi. Alcuni esempi:

Reati informatici
La legge 547/93 individua e vieta una serie di comportamenti nell'ambito informatico che sono stati reputati lesivi per gli interessi non solo di singoli privati cittadini, ma anche di persone giuridiche, in particolare per le imprese e gli enti pubblici:
• Accesso abusivo ad un sistema informatico e telematico
Attività di introduzione in un sistema mediante il superamento di chiavi "fisiche" o logiche poste a protezione di quest'ultimo (Art. 615 ter cp).
Per commettere il reato basta il superamento della barriera di protezione del sistema o accedere e controllare via rete un PC all' insaputa del legittimo proprietario, oppure forzare la password di un altro utente e, più in generale, accedere abusivamente alla posta elettronica, ad un server o ad un sito cui non siamo autorizzati.
• Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico
L'art 615 quinquies punisce "chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri creato, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento".
Per commettere questo reato basta, anche solo per scherzo, diffondere un virus attraverso il messenger o la posta elettronica, spiegare ad altre persone come si può fare per eliminare le protezioni di un computer, un software o una console per giochi oppure anche solo controllare a distanza o spegnere un computer via rete.

• Danneggiamento informatico

-Per danneggiamento informatico si intende un comportamento diretto a cancellare o distruggere o deteriorare sistemi, programmi o dati. L'oggetto del reato, in questo caso, sono i sistemi informatici o telematici, i programmi, i dati o le informazioni altrui. Art. 635 cp.

• Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

Questo particolare reato viene disciplinato dall'art. 615 quater cp e si presenta spesso come complementare rispetto al delitto di frode informatica.

• Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici

E' considerato reato anche quando l'informazione viene carpita in modo fraudolento con "inganni" verbali e quando si prende conoscenza diretta di documenti cartacei ove tali dati sono stati riportati, oppure osservando e memorizzando la "digitazione" di tali codici.

Si commette questo reato quando si carpiscono, anche solo per scherzo, i codici di accesso alla posta elettronica, al messenger o al profilo di amici e compagni.

• Frode informatica

Questo reato discende da quello di truffa e viene identificato come soggetto del reato "chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità sui dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno". Art. 640 ter cp.

Il profitto può anche "non avere carattere economico, potendo consistere anche nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale".

Il delitto di frode informatica molto sovente viene a manifestarsi unitamente ad altri delitti informatici, quali l'Accesso informatico abusivo e danneggiamento informatico in conseguenza a Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

Reati non informatici

Sono da considerare reati non informatici tutti quei reati o violazioni del codice civile o penale in cui il ricorso alla tecnologia informatica non sia stato un fattore determinante per il compimento dell'atto:

• Ingiuria

Chiunque offende l'onore o il decoro di una persona presente commette il reato di ingiuria.

Incorre nello stesso reato chi commette il fatto mediante comunicazione telegrafica o telefonica o con scritti, o disegni, diretti alla persona offesa.

• Diffamazione

Qualcuno che offende la reputazione di qualcun altro, quando all'interno di una comunicazione con più persone si diffondono notizie o commenti volti a denigrare una persona. Art. 595 cp. Aggravante nel caso in cui l'offesa sia recata con un "mezzo di pubblicità" come l'inserimento, ad esempio, in un sito Web o social network di una informazione o un giudizio su un soggetto. La pubblicazione on-line, dà origine ad un elevatissimo numero di "contatti" di utenti della Rete, generando una incontrollabile e inarrestabile diffusione della notizia.

• Lesione del Diritto d'autore

Un primo caso di violazione del diritto d'autore si può verificare quando una copia non autorizzata di un'opera digitale è caricata su un server e messa a disposizione degli utenti. In questo caso, colui che riproduce e fornisce l'opera senza l'autorizzazione da parte del suo autore è considerato soggetto responsabile. Per commettere questo reato basta pubblicare su YouTube un video con una qualsiasi musica di sottofondo senza le dovute autorizzazioni.Un'ulteriore possibile violazione del diritto d'autore si verifica quando l'utente ottiene il documento, il software o il brano mp3 messo a disposizione in rete o acquistato e ne fa un uso illegittimo, come ad esempio, rivenderlo a terzi o distribuirlo sulla Rete facendone più copie non autorizzate.

La legge italiana sul diritto d'autore consente all'utilizzatore di un software o di un opera multimediale o musicale di effettuare un'unica copia di sicurezza ad uso personale, utile nei casi di malfunzionamento del programma, smarrimento della copia originale etc. Tale copia, salvo autorizzazione della casa di produzione, non può essere ceduta ad altre persone.
La duplicazione abusiva (senza autorizzazione) è sanzionata penalmente e colpisce ugualmente anche chi duplica abusivamente non a scopo di lucro, bensì per un semplice fine di risparmio personale.

Policy di sicurezza informatica in uso presso il Liceo Visconti

In applicazione delle norme di sicurezza che tutelino tutta la comunità scolastica, il sistema di accesso ad internet della scuola - il cui Amministratore di rete, incaricato dal Dirigente scolastico è il sig. Emanuele Loi, tecnico esperto della Società Roma Libri & Informatica, in collaborazione con l'A.T. della scuola Daniele Esposito - prevede l'uso di un filtro per impedire l'accesso a contenuti non compatibili con la politica educativa della scuola (sesso, violenza, droghe, comportamenti criminali, occultismo, appuntamenti ed incontri, giochi d'azzardo, ecc.).

Dal punto di vista tecnico l'accesso ad internet viene gestito da un componente di rete attivo (firewall Sophos USG220) in grado di gestire il traffico di rete in modo sicuro e intelligente grazie alle seguenti funzionalità:

- Difesa attiva contro le intrusioni
- Blocco del traffico in uscita diretto agli host dei centri di comando e controllo e alle Botnet
- Deep Packet Inspection con oltre 18.000 definizioni
- Protezione antiflood (DoS, DDoS, scansione delle porte) per la rete
- Supporto di SSL, IPsec
- AES/3DES a 256 bit, PFS, RSA, certificati x.509, chiavi precondivise
- Autenticazione sicura per gli utenti
- Sophos Authentication Agent per gli utenti
- Supporto di Active Directory, eDirectory, RADIUS, LDAP, TACACS+
- Autenticazione a due fattori che utilizza una one-time password (OTP), ad es. per Portale Utenti, IPSec, SSL VPN, senza alcun bisogno di altre infrastrutture

La funzionalità di filtraggio Advanced Threat Protection fornisce un unico riquadro per l'individuazione e il blocco di tutti gli attacchi all'interno della rete, persino quelli più mirati. Il rilevamento dei sistemi utilizzati dai centri di comando e controllo e delle Botnet, unito ai pattern IPS e Deep Packet Inspection, consente di individuare e bloccare probe e attacchi rivolti ad applicazioni e protocolli.

Il vasto database delle signature dei SophosLabs contiene moltissimi pattern e regole e si aggiorna ogni pochi minuti e grazie alla funzione sandboxing in-the-cloud per l'analisi dei file sconosciuti e dei contenuti malevoli si garantisce il continuo miglioramento della protezione da malware, spyware e/o virus che vengono bloccati prima di riuscire a raggiungere la rete grazie ai due motori di scansione antivirus indipendenti.

Il dispositivo ha una protezione comprovata contro le minacce Web e i nuovi metodi di raggiramento degli utenti rilevando e bloccando con tecniche avanzate quali emulazione di JavaScript e ricerche in-the-cloud di Live Protection, per rilevare il codice Web malevolo prima che riesca a raggiungere il browser. Inoltre, viene impedito ai sistemi infetti di effettuare il call home e inviare dati di natura sensibile. Tramite il motore di analisi viene processato tutto il traffico HTTP,

HTTPS, FTP, SMTP e POP3, con l'inclusione di contenuti attivi come Active X, Flash, cookie, VBScript, Java e JavaScript.

La funzionalità URL Filtering agisce tramite Transparent Proxy integrato che effettua l'ispezione dei pacchetti in transito ricostruendo gli instradamenti e analizzando i contenuti, confrontandoli con il database dei SophosLab, che viene aggiornato in maniera costante e contiene oltre 35 milioni di siti, suddivisi in 96 categorie, in modo da applicare policy specifiche. Ciò rende possibile la creazione facile e veloce di policy di navigazione sicura, minimizzando i potenziali rischi legali relativi a eventuali contenuti inadeguati e mantenendo in sicurezza tutte le postazioni.

La policy predefinita dell'url filtering è basata sul concetto di blacklist e whitelist provvedendo ad una limitazione nel caso in cui il contenuto identificato nei pacchetti in transito abbia una corrispondenza con le categorie e i pattern presenti nel database.

La procedura di analisi è completamente automatizzata e a volte può identificare dei falsi positivi che, se comunicati al Dirigente, verranno analizzati, valutati e inseriti in whitelist per consentirne l'accesso da parte degli utenti.

Ad esempio, si è verificato nel liceo il caso di banner o porzioni di codice javascript all'interno delle pagine come per le webmail micso/alice/libero; comunicata la problematica di accesso e/o malfunzionamento della pagina da parte dei docenti interessati, è stata prontamente creata una policy per la risoluzione della problematica.
Un ulteriore esempio ha riguardato la sottocategoria "revisionismo storico" presente in una delle macro categorie di default che inibiva la visualizzazione di siti utili alla didattica del liceo, anch'essa resa disponibile dopo segnalazione e valutazione.

Al momento sono in funzione i seguenti filtri per categoria e alcune policy di bypass create appositamente da segnalazioni ricevute:

Attività criminali
- Exploit del browser
- Attività criminali
- Hacking/Crimini informatici
- Odio-diffamazione/Discriminazione
- Software illegale
- Illegal UK
- Download maligni
- Programmi potenzialmente indesiderati
- Informazioni su frodi scolastiche

Nudità
- Nudità
- Pornografia
- Bestemmie
- Materiale a contenuto sessuale

Sospetto
- Spyware/Adware
- Dominio parcheggiato

- Siti maligni
- URL di spam
- Pubblicità sul web
- Phishing

Videogame / giochi d'azzardo

- Contenuti per bambini
- Giochi
- Gioco d'azzardo
- Contenuti correlati al gioco d'azzardo

Eccezioni con autenticazione:
alice.it webmail
libero.it webmail
micso.it webmail

Eccezioni senza autenticazione:
tutti i servizi google (comprese funzioni google android)
servizi argo per registro elettronico
url specifiche di software ad uso comune per consentire gli aggiornamenti (es. avg, windows update, mozilla, ecc.).

Qualsiasi segnalazione utile al miglioramento del servizio è auspicata.
Come già detto, il Dirigente Scolastico può autorizzare la navigazione di siti leciti ai fini scolastici che, per qualsiasi motivo, risultino inaccessibili, su segnalazione scritta e motivata dell'interessato.

IL DIRIGENTE SCOLASTICO
Prof.ssa Clara Rech