Collini Consulting s.a.s.
via Cervese, 1424
47521 Cesena (FC)
tel. +39 0547 632314
fax +39 0547 635019
www.flashstart.it

LA SICUREZZA NELLE SCUOLE

una scelta responsabile verso gli Studenti e le Famiglie

Grazie alla nostra esperienza maturata in oltre 15 anni di attività al servizio delle Scuole italiane con i prodotti della linea "FlashStart", ci confrontiamo ogni giorno con Dirigenti scolastici, DSGA ed amministratori di Rete. Ascoltiamo le loro esigenze e cerchiamo di sviluppare le soluzioni idonee al mondo della Scuola.
La Normativa italiana è chiara ed inequivocabile e richiede al Dirigente - e ai suoi collaboratori - un grande impegno al fine di tutelare i ragazzi dal grave fenomeno del Cyberbullismo e proteggerei dati presenti negli archivi scolastici.
Riferimenti normativi:

- Direttiva 16/2007 (Cyberbullismo)
- Decreto Legge 159/2007 (Direttiva "Brunetta")
- Decreto Legge 196/2003 (Privacy) e successive modifiche
- G.U. 300 del 24/12/2008 con le misure prescritte agli amministratori di sistema.

Di seguito abbiamo riassunto, in paragrafi distinti, le caratteristiche normative, tecniche ed operative che a nostro avviso dovrebbero essere essenziali per la Scuola al momento della richiesta di qualunque progetto/preventivo che riguarda la "sicurezza delle reti LAN".

RISPETTO DELLA NORMATIVA E DELLE MISURE RICHIESTE DALLA LEGGE

- rispetto della Direttive Ministeriali 16/2007 al fine di limitare al massimo i rischi online derivanti da eventi di Cyberbullismo
- tracciabilità totale degli accessi registrati su sistema di memorizzazione idoneo, con backup a norma di Legge (196/2003)
- profilazione e tracciamento degli accessi alle funzioni di amministrazione del Firewall da parte dei tecnici/amministratore di rete (G.U. 300 del 24/12/2008). Sono necessari più livelli di azione, con logging delle operazioni fatte dal singolo amministratore e possibilità di personalizzazione "granulare" sulle configurazioni
- stampa automatica delle lettera di consegna delle credenziali da consegnare a Studenti/Famiglie, su carta intestata della Scuola e con regolamento dell'utilizzo della rete Internet

AUTENTICAZIONE DEGLI UTENTI

- adozione di un sistema di accesso ad internet autenticato da username e password personali al fine di garantire il Dirigente Scolastico da eventuali illeciti commessi dai propri utenti su internet;
- implementazione di un sistema di autenticazione che prevede, all'apertura del programma di navigazione, una pagina "Captive Portal" con l'inserimento delle proprie credenziali che saranno utilizzate dal sistema per associare il corretto profilo (studenti, insegnanti, personale amministrativo, ecc.), con differenti restrizioni e politiche di navigazione;
- per le Scuole multiplesso, attuazione di un sistema di autenticazione centralizzato nella Sede principale in grado di gestire le richieste di accesso provenienti dalle Sedi periferiche in modo da garantire la circolarità degli utenti (si pensi ad un insegnante che deve svolgere lezioni in più plessi scolastici), su una unica base dati condivisa;

Collini Consulting s.a.s.
via Cervese, 1424
47521 Cesena (FC)
tel. +39 0547 632314
fax +39 0547 635019
www.flashstart.it

- memorizzazione nel disco SSD presente localmente degli accessi log degli eventi, a disposizione per verifiche e controlli (il disco SSD per i log è basilare nel firewall)
- salvataggio tramite idoneo sistema di backup degli access log su supporto esterno;
- supporto per le postazioni connesse via rete LAN ed per i dispositivi Mobile (tablet, smartphone, laptop, ecc.) connessi mediante le reti Wifi scolastiche;
- procedura di caricamento rapido dai principali software gestionali scolastici mediante esportazione in Excel e deve essere anche in grado di generare automaticamente la login e password;
- possibilità di impostare sessioni "a tempo" o "tramite pop-up";
- scollegamento rapido degli utenti al cambio dell'ora nei Laboratori;
- supporto per sincronizzazione con Microsoft Active Directory per le reti che fossero dotate di apposito Server, in modo da utilizzare la base dati Active Directory

FILTRO CONTENUTI E PROFILAZIONE DIFFERENZIATA DEGLI UTENTI

- Creazione dinamica di differenti profili di navigazione per tipologia di utente (studenti, insegnanti, impiegati, dirigenti, ecc.), ognuno con le sue limitazioni e concessioni;
- Rimozione delle limitazioni al personale tecnico preposto alla manutenzione dei laboratori per permettere loro lo svolgimento degli aggiornamenti e delle installazioni;
- Blacklist di sistema categorizzate per tema, pericolosità, gruppo e macrogruppo
- Possibilità di inserire blacklist e whitelist personalizzate per gruppo di utenza
- Aggiornamento continuo delle liste
- Catalogazione proattiva entro 24 ore delle nuove minacce, basato sull'analisi quotidiana dei siti visitati dagli utenti FlashStart e non ancora censiti
- Profilazione e limitazioni per download (files e mime)
- Sensore personalizzabile per analisi semantica dei contenuti
- Gestione filtro "ad orari"
- Antivirus sulla navigazione
- Proxy trasparente oppure esplicitato su browser con funzione WPAD

RISPETTO DELLA DIRETTIVA 16/2007 SUL CYBERBULLISMO

- rispettare appieno le Direttive Ministeriali al fine di limitare al massimo gli eventi online legati al tema del Cyberbullismo;
- tracciabilità totale degli accessi registrati su sistema di memorizzazione idoneo, con backup a norma di Legge (196/2003);
- stampa automatica delle lettera di consegna delle credenziali da consegnare a studenti/famiglie, su carta intestata della Scuola e con indicato il regolamento dell'utilizzo della rete Internet

RISPETTO DELLE REGOLE "AMMINISTRATORI DI SISTEMA" (G.U. 300 del 24/12/2008)

- accesso al Firewall da parte degli amministratori di sistema, e collaboratori tecnici designati, mediante una login personale;
- creazione di più profili "amministrativi" con scelta peculiare e granulare delle funzionalità da abilitare ad ogn amministratore di sistema (es. selezione delle blacklist, blocco di gruppi di computer, gestione delle regole firewall, ecc.);

Collini Consulting s.a.s.
via Cervese, 1424
47521 Cesena (FC)
tel. +39 0547 632314
fax +39 0547 635019
www.flashstart.it

- tracciamento e morizzazione su disco SSD delle operazioni fatte dai singoli amministratori, come richiesto dalla G.U. 300 del 24/12/2008

DNS PROXY "BLACKHOLE" (per rafforzamento filtraggio applicazioni ed altri protocolli)

- attivazione di un proxy e filtro mandatorio delle richieste DNS;
- possibilità di attivazione a scelta su utenti/gruppi/ip;
- inibizione della risoluzione DNS per i siti presenti nelle blacklist selezionate;
- blocco "on dns resolution" dei siti https e delle applicazioni mobile che utilizzano la risoluzione dei nomi;
- funzionamento indipendente da sistema di deep inspection https e rewrite del certificato di sicurezza (da noi sconsigliato anche in base a potenziali "violazioni di Legge" di questa tecnica utilizzata da prodotti concorrenti: https://epic.org/privacy/dpi/)
- integrazione DNS Proxy con Server di dominio "Active Directory"

REPORT PRIVACY-COMPLIANT

- analisi del traffico ad internet per tipologia di traffico, per categoria di sito, per orario, per tipologia di download e per nazione/continente visitato;
- report di traffico in linea con le disposizioni in materia di Privacy e in rispetto dello Statuto dei Lavoratori: nessun dato personale ma unicamente informazioni aggregate, che non permettano di risalire in alcun modo alle preferenze di navigazione dei singoli utenti ed essere quindi lesive alla Privacy delle persone;
- reportistica visibile solo nell'area web riservata di gestione del Firewall con possibilità di ricezione in posta elettronica della reportistica PDF, differenziata per tipologia di utente (Dirigente, DSGA, tecnici, ecc.)

PROTEZIONE DELLE "RICERCHE E IMMAGINI DI GOOGLE"

- sistema di content filtering in grado di lasciare visualizzare soltanto i risultati consoni all'attività didattica e lavorativa inibendo materiali audio e video indesiderati;
- funzionamento integrato della "Safe search" di Google in modalità mandatoria

FUNZIONALITA' FIREWALL E DI BASE

- protezione del perimetro di rete e corretta gestione del traffico da e verso Internet;
- firewall in grado di selezionare le porte ed i servizi da concedere e da bloccare;
- firewall unico, e dinamico, con differenti regole da applicare agli utenti della Segreteria e della Didattica e con possibilità di policy diverse a seconda dei gruppi di autentica;
- funzionalità di routing statico, DNS, DHCP, NAT/PAT;
- funzionalità DMZ;
- accesso web e console all'apparato FlashStart;
- funzione virtual server;
- supporto VLAN;
- Sistema di monitoraggio "in Cloud" integrato con centrale operativa;

Collini Consulting s.a.s.
via Cervese, 1424
47521 Cesena (FC)
tel. +39 0547 632314
fax +39 0547 635019
www.flashstart.it

- Backup delle configurazioni remote “in Cloud” integrate con storico di almeno 30 giorni;
- Punti di ripristino ad “intervalli orari” per un veloce ritorno a configurazioni precedenti;
- Ripristino rapido in “5 minuti” tramite “backup-in-cloud”;
- Funzione di aggiornamentp clock via NTP;
- DHCP, DNS, routing statico

MONITORAGGIO REMOTO PROATTIVO

- sistema di sicurezza internet in funzione 24 ore su 24 e 7 giorni su 7, per proteggere gli accessi degli utenti e bloccare le minacce provenienti dall'esterno;
- sistema di monitoraggio “in Cloud” del Produttore in grado di verificare H24 le funzionalità vitali della macchina Firewall, allertando in csao di anomalie e malfunzionamenti sulla Rete;
- il sistema di monitoraggio deve prevedere un accesso web per gli Amministratori di Rete che consenta la verifica in tempo reale dello stato della propria rete e la conseguente apertura di richieste di supporto.

SUPPORTO TECNICO E TRACCIAMENTO DEGLI INTERVENTI

- helpdesk disponibile almeno dalle ore 8.30 di mattina alle ore 18.30 di sera, in italiano e con operatori madrelingua;
- inoltro delle richieste di assistenza tecnica tramite: call center, sito web, email e SMS (strumento rapido e importantissimo);
- tracciamento delle richieste e degli interventi online tramite un’interfaccia con lo stato in tempo reale (Tracking) delle proprie richieste (aperta, in gestione, chiusa) e la possibilità di leggere le soluzioni ed interagire con i tecnici

GEOLOCALIZZAZIONE E BLOCCO DEI PAESI INDESIDERATI

- attivazione del modulo di geolocalizzazione, in grado di bloccare il traffico dai Paesi a rischio infezioni e pirati informatici (se un Ente ha esigenze standard di navigazione, basterà abilitare il traffico verso l'Europa e il Nord America dove risiedono i più importanti siti mondiali quali Google, Microsoft, ecc. e bloccare tutto il resto: le possibilità di attacco da hacker, virus, spyware, ecc. diminuirà esponenzialmente, bloccando a monte le fonti considerate non sicure a livello di internet)

GESTIONE DI PIU' CONNESSIONI AD INTERNET

- gestione di almeno 2 porte WAN con la distribuzione del carico per utente, profilo, ip;
- gestione di più connessioni LAN con distribuzione della connettività personalizzabile;
- failover automatico della connettività in caso di indisponibilità di una o più direttrici

Collini Consulting s.a.s.
via Cervese, 1424
47521 Cesena (FC)

tel. +39 0547 632314
fax +39 0547 635019
www.flashstart.it

PROTEZIONE DELLA POSTA ELETTRONICA

- protezione da virus e spyware della corrispondenza email, data l'alta sensibilità dei dati contenuti negli archivi di Segreteria;
- gestione trasparente ed automatica della protezione antispam e blocco delle email infette, in apposita quarantena;
- protezione "relay-postale" per le Scuole che hanno un server di posta elettronica interno all'Istituto

SOFTWARE IN ITALIANO E A PIU' LIVELLI DI GESTIONE

- pannello di amministrazione semplice e fruibile in italiano, cosi come la guida rapida e la manualistica in linea;
- disponibilità di più livelli amministrativi, concessi in delega parziale dall'Amministratore di Rete ai propri collaboratori, profilando per ogni modulo (firewall, filtro, autentica, ecc.) i permessi di visualizzazione, gestione o inibizione;
- ogni utente, per la Direttiva sugli Amministratore di sistema, deve potere accedere allo strumento Firewall con le proprie credenziali e le modifiche alla configurazione devono essere tracciate.

PROTEZIONE E GARANZIA DELL'INVESTIMENTO

- disponibilità di un periodo di garanzia, aggiornamenti e supporto almeno per 24 o 36 mesi dalla data di acquisto del prodotto;
- continuità nello sviluppo della soluzione almeno per i prossimi 48 mesi;
- installazione ed aggiornamento automatico delle nuove blacklist, funzionalità e migliorie