ISTITUTO CAPIROLA DI LENO (BS)

SESSIONE FORMATIVA USO CONSAPEVOLE SICURO E LEGALE DELLA RETE

Mauro Ozenda

Email: mauro.ozenda@gmail.com)

Agenda

- Regolamento informatico interno, Netiquette
- I rischi della rete
- Modalità comportamentali e consigli
- Utilizzo delle liberatorie utilizzo di internet e immagini minori

Rete LAN segreteria

- Rete Interna (server di rete armadio– postazioni client – apparati attivi di rete – collegamento a internet)
- Server di rete: dati gestiti centralmente (salvataggio dati giornaliero su hard disk esterno)
- Connessione a internet condivisa
- Posta elettronica e gestione fax
- Periferiche condivise sulla rete

Gestione ACCOUNT

- Attivazione n° xx account con policy autorizzazione accesso ai programmi e alle cartelle conformi all'attività di competenza;
- Diritti amministrativi al DSGA e D.S.
- Password con diritti illimitati al D.S. (titolare trattamento dei dati) e all'amministratore di sistema che svolge l'attività di assistenza
- La pwd rimane in possesso esclusivo dell'utente che l'attiva
- Lanciare SALVASCHERMO protetto da pwd ogni qualvolta si abbandona la propria postazione

SICUREZZA FISICA

- ARMADIO APPARATI ATTIVI DI RETE (switch e router)
- ARMADIO SERVER DI RETE
- GRUPPI DI CONTINUITA' SERVER, APPARATI ATTIVI E SINGOLE POSTAZIONI
- PORTA CPU SU OGNI SINGOLA POSTAZIONE

SICUREZZA LOGICA

- ANTIVIRUS: configurato antivirus centralizzato aggiornato automaticamente via web;
- FIREWALL: verifica firewall MS WINDOWS 2003 SERVER
- AGGIORNAMENTI: configurato aggiornamenti automatici centralizzati sul server sia del sistema operativo di rete che dell'antivirus (patch di sicurezza);
- SALVATAGGIO DATI: salvataggio dati a cadenza giornaliera in notturna (dal lunedì al sabato ore 22:00);
- **WOT/MCAFEE SITE ADVISOR**: per l'attendibilità di un sito web;
- PORTE USB E DVD: disabilitato sulle singole postazioni

ASSISTENZA TECNICA SISTEMA INFORMATICO(consigli)

- In OUTSOURCING mediante liberatoria con possibilità di teleassistenza (collegamento in remoto dall'esterno);
- Manutenzione programmata periodica sui singoli PC
- Verifica periodica avvenuto aggiornamento sistemi operativi di rete e in locale
- Verifica periodica avvenuto salvataggio dei dati con inoltro ALERT nel caso in cui per qualche motivo non vengano effettuati
- Verifica periodica aggiornamenti antivirus centralizzato lato server e lato client.

Disciplinare Tecnico

Codice etico della rete (Netiquette)

- **Rispettare la privacy**
  Usare in rete la stessa regola che usi nella vita. Ognuno di noi ha il diritto di scegliere se condividere o meno le informazioni che lo riguardano.

  Essere prudente
  Non dare in modo affrettato informazioni personali o che riguardano la propria famiglia. Non accettare senza riflettere di incontrare qualcuno che si è appena
  conosciuto nella rete. Non credere a tutto quello che viene detto.

- **Trascurare gli errori degli altri**
  Il desiderio di rispondere velocemente porta a errori di digitazione, di grammatica o
  di sintassi **ma l'importante è che il messaggio sia compreso**.

- **Non urlare**
  Scrivere in maiuscolo su Internet equivale ad urlare: è uno strumento a disposizione per enfatizzare le cose che stai dicendo. Attenzione a non abusarne.

Principali regole buona educazione virtuale

EMAIL

- Inserire sempre l'oggetto nelle email che spediamo per agevolare la gestione di chi le riceve

- Se si manda un messaggio a più destinatari occorre non indicare gli indirizzi nello spazio del destinatario (A) ma indicarli solo in copia per conoscenza (cc) o in copia nascosta (CCn) rispettando anche le normative sulla privacy

- Non usare i caratteri tutti in maiuscolo nel titolo o nel testo dei tuoi messaggi, nella rete questo comportamento equivale ad "urlare" ed è altamente disdicevole

MODALITA' COMPORTAMENTALI E CONSIGLI

CREDENZIALI DI AUTENTICAZIONE

- **Usiamo 14 caratteri, con caratteri maiuscoli, caratteri speciali e con numeri (pwd efficace) non riconducibile a dati personali né parole presenti nel vocabolario;**
- **Abituiamoci alla "gelosia" nei confronti delle password**
- **Abituiamoci a custodire in luogo sicuro tutte le password**
- **Modificarle periodicamente e ogni qualvolta si ha il minimo dubbio che possa esser stata carpita da altri**
- **Per i diversi servizi utilizzati (emai,remote banking,etc) utilizzare pwd diverse e non sempre la stessa**
- **Installare Keepass Password Safe per gestione pwd**

PASSWORD

- **AMMINISTRATORE DI SISTEMA: password in possesso del tecnico sistemista che segue l'assistenza del sistema informatico della scuola;**
- **TITOLARE TRATTAMENTO DEI DATI: password in possesso del DIRIGENTE SCOLASTICO che può controllare anche l'operato dell'amministratore di sistema (log attività);**
- **SINGOLI ACCOUNT: ogni utente ha una sua password per accedere alle funzionalità che gli sono state assegnate;**
- **ROUTER: la password del router deve essere modificata e custodita in cassaforte dal DIRIGENTE SCOLASTICO.**

Protezione PC e Rete Informatica

- **Non installate software superfluo o di dubbia provenienza**
- Non aprite **gli allegati non attesi**, di qualunque tipo
- **Non fidatevi dei LINK a banche o negozi forniti da sconosciuti**. Possono essere falsi o portarvi ad un sito truffa (**phising/pharming**)
- **Non distribuite documenti di word o excel**: trasportano virus e contengono vostri dati personali nascosti. Inviate in allegato solo files in formato compresso (**zip-rar**) o in **formato Adobe Pdf protetto da scrittura**.
- Non collegatevi da computer pubblici a siti con accesso a dati riservati (pericolo Keylogger).

PUA: utilizzo del software

- I **software** installati sono ad **esclusivo uso didattico**. Chiunque abbia bisogno di aggiornamenti o nuovi applicativi da acquistare deve farne richiesta al Responsabile.

- **E' fatto divieto di usare software non conforme alle leggi sul copyright**. E' cura dell'insegnante-utente di verificarne la conformità. Gli insegnanti possono installare nuovo software sui PC del laboratorio previa autorizzazione scritta del Referente di laboratorio. Si raccomanda, quindi, di verificare che il software installato rispetti le leggi sul copyright.

PUA: accesso ad internet

- L'accesso a Internet è consentito al personale docente e non docente solo ad **esclusivo uso didattico e/o di formazione e alle classi** accompagnate e sotto la responsabilità di un insegnante.

- **E' vietato** inserire sui Pc connessi in rete **programmi contenenti virus**, scaricare software non autorizzati da internet, scaricare e **installare software senza licenza.**
- **E' vietato scaricare musica, immagini o video coperti da diritto d'autore** se non previo autorizzazione scritta da parte dell'autore/casa editrice.

Pubblicazione sito web della scuola

- Nella pubblicazione di immagini degli alunni è necessaria la **preventiva liberatoria da parte dei genitori** o da chi ne esercita la funzione.

- Anche in presenza di liberatoria da parte dei genitori la scuola procederà con la massima attenzione, **preferendo pubblicare immagini a campo lungo, senza primi piani; immagini di gruppo in attività piuttosto che di singoli**; in alcuni casi sarà opportuno "sfocare" un po' i volti degli alunni.

- La scuola non pubblicherà materiale prodotto dagli studenti senza il permesso dei loro genitori.

Liberatorie Genitori per l'utilizzo delle immagini/video dei minori

INFORMATIVA/LIBERATORIA:

- Per l'utilizzo degli strumenti informatici e per l'accesso ad internet nel laboratorio informatico da parte dei minori
- Per l'utilizzo di immagini e video che riprendono i ragazzi della scuola con inserimento sul portale web della scuola e la creazione di DVD ad uso scolastico
- Per la pubblicazione sul web dei lavori svolti dai ragazzi per i quali la scuola è detentrice dei diritti
- Informativa utilizzo delle immagini/video durante eventi della scuola solo ad un uso strettamente personale e non divulgativo.

I Fake


Microsoft: in una settimana un milione di PC attaccati dai virus | oneITsecurity - Windows Internet Explorer
http://www.oneitsecurity.it/26/11/2008/microsoft-in-una-settimana-un-milione-di-pc-attaccati-dai-virus/
File Modifica Visualizza Preferiti Strumenti ?
Microsoft: in una settimana un milione di P...
Pagina Strumenti
Microsoft: in una settimana un milione di PC attaccati dai virus
di Gianluca Rini - Mercoledì 26 Novembre 2008 alle 15:04
Microsoft
Da un post in un blog di Microsoft si apprende la notizia che nella settimana tra l'11 e il 19 novembre quasi un milione di PC è stato preso d'assalto da numerosi virus, il cui numero è stato in forte aumento. Questi virus hanno raggiunto i PC attraverso l'ormai consueto sistema di mascheramento del malware sotto le "mentite spoglie" di software per la sicurezza. Le tracce di questi falsi antivirus sono state rilevate dal Malicious Software Removal Tool (MSRT).
I virus riconosciuti dal Malicious Software Removal Tool appartengono ad una stessa famiglia di malware chiamata Win32/FakeSecSen. Fra questi virus ricordiamo alcuni antivirus falsi, come MS Antivirus, Spyware Preventer, Vista Antivirus 2008, Power Antivirus.
Il piano messo in atto dagli fake antivirus è lineare e allo stesso tempo efficace: essi si propongono all'utente come dei programmi antivirus gratuiti, in grado di effettuare un controllo sul PC, per verificare se sia infetto. Poi, una volta attivati, fanno visualizzare falsi messaggi, che informano l'utente che il suo PC presenta dei virus.
A questo punto l'utente è invitato ad acquistare online un non meglio specificato update del prodotto e il gioco è fatto. Per rendere il tutto più credibile i nomi dei virus, così come i loro loghi e le loro interfacce sono creati ad hoc per assomigliare a quelli dei prodotti più famosi nell'ambito della sicurezza.
Come chiarisce Microsoft, in ogni installazione di FakeSecSen sono contenuti: un programma eseguibile, uno o due file DAT, un'applicazione che ha l'obiettivo di linkare il falso antivirus al pannello di controllo di Windows e una scorciatoia sul desktop; a volte si trova anche un falso uninstaller. La famiglia FakeSecSen ha insomma tutte le carte in regola per
La stampa ecocompatibile costa meno. Anche all'ambiente.
Offerta limitata nel tempo: Kit di Stampa Ecocompatibile con ogni stampante a colori Phaser™ 8560.
risparmia subito
RSS oneITsecurity / commenti
NETWORK Ultimi post del network
NEWSLETTER tua@email
iscriviti
COLLABORARE? Inviaci una segnalazione
ULTIMI POST DEL NETWORK
CATEGORIE
Aggiornamenti software
Eventi
Exploit e bug
Leggi
Malware
Novità e tendenze
Phishing
Produttori
Sicurezza
Sistemi di protezione
Spam
COMMENTI RECENTI
RK in Obama e McCain, entrambi sotto l'attacco degli hacker
Gianluigi in Problemi con MSN Messenger? Non preoccupatevi, c'è Live Kill
Ratamusa in Iran, è a rischio vivere da blogger
sara in Problemi con MSN Messenger? Non preoccupatevi, c'è Live Kill
riccardoo in Problemi con MSN Messenger? Non preoccupatevi, c'è Live Kill
Internet
100%

Trovi un PENDRIVE : COSA FARESTI ?

Verifiche in stand bye

1. Creazione 3 account con privilegi di amministratore con pwd differenziate
2. Possibilità gestione fax server centralizzato
3. Collegamento sistema wi-fi dell'istituto mediante autenticazione account via proxy
4. Installazione WSUSE lato server (http://technet.microsoft.com/it-it/windowsserver/bb332157.aspx)
5. Modificare PUA inserendo possibilità utilizzo pendrive in laboratorio prevedendo disabilitazione autorun e verifica sistemi di controllo malware (antivirus)
6. Gruppi continuità e porta cpu per ogni mini-tower della segreteria
7. Verifica sistemi di crittografia sulle cartelle
8. Scarico keepass password safe per generare/salvare pwd
9. Password ROUTER (custodire in cassaforte, a conoscenza del solo titolare trattamento dei dati)

ISTITUTO CAPIROLA DI LENO (BS)

SESSIONE FORMATIVA USO CONSAPEVOLE SICURO E LEGALE DELLA RETE

Mauro Ozenda

Email: mauro.ozenda@gmail.com)