Arch. Spaccini Gianfranco

sito web - http://www.spaccini.net
email - spaccini.dirigente@gmail.com

GIOVANI & WEB

Software di controllo e programmi filtro

Internet e la Sicurezza informatica: suggerimenti per la sicurezza

Quanta della vs vita quotidiana si affida ai computer?
Quante delle Vs informazioni personali sono memorizzate sul Vs PC o di qualcuno? e… Dove?

- Comunicazione (email, cellulari..)
- Intrattenimento (filmati digitali, mP3..)
- Trasporto (automobile, aereo, GPS..)
- Acquisti (negozi on-line, carta credito, transazioni..)
- Medicina (documentazione, attrezzature..)

Quando si parla di sicurezza si deve far riferimento a due concetti: Sicurezza come certezza, attendibilità, garanzia di avere a disposizione le informazioni sempre e verificate; Sicurezza come salvaguardia, incolumità dei nostri dati e delle nostre apparecchiature.

Scopo Della Sicurezza Informatica

Misure organizzative, tecnologiche, procedurali
Misure di protezione:

- Prevenzione
- Individuazione (quando, come, chi)
- Reazione

Requisiti Della Sicurezza (disponibilità, integrità, riservatezza, autenticità e non ripudio)

- Capire i rischi
- Significato dei termini base
- Cosa fare per proteggersi

Malware *(programma malvagio o codice maligno)*

- Virus > codice maligno > hanno bisogno di file > richiede azione utente
- Worms > non bisogno file > modificano O.S. > no azione utente (Conficker) **Microsoft Malicious Software Removal Tool**
- Trojan horses > software (Alanchum.VL - *Cimuz.BE,* Kenzero*)*
- Backdoor > software > worms, trojan (Back Orifice, Gola Profonda)

Hacker, Cracker, Attacker, Intruder, Phisher, Botmaster…

Spyware *(TomCat),* **Adware, Cookie** *(SpyBot Search&Destroy, Ad_aware)*

Sfatare I Miti

- AV e firewall ci proteggono al 100%
- Una volta installato un software non mi devo preoccupare di altro *(patch)*
- Non ho niente da proteggere *(spam)*

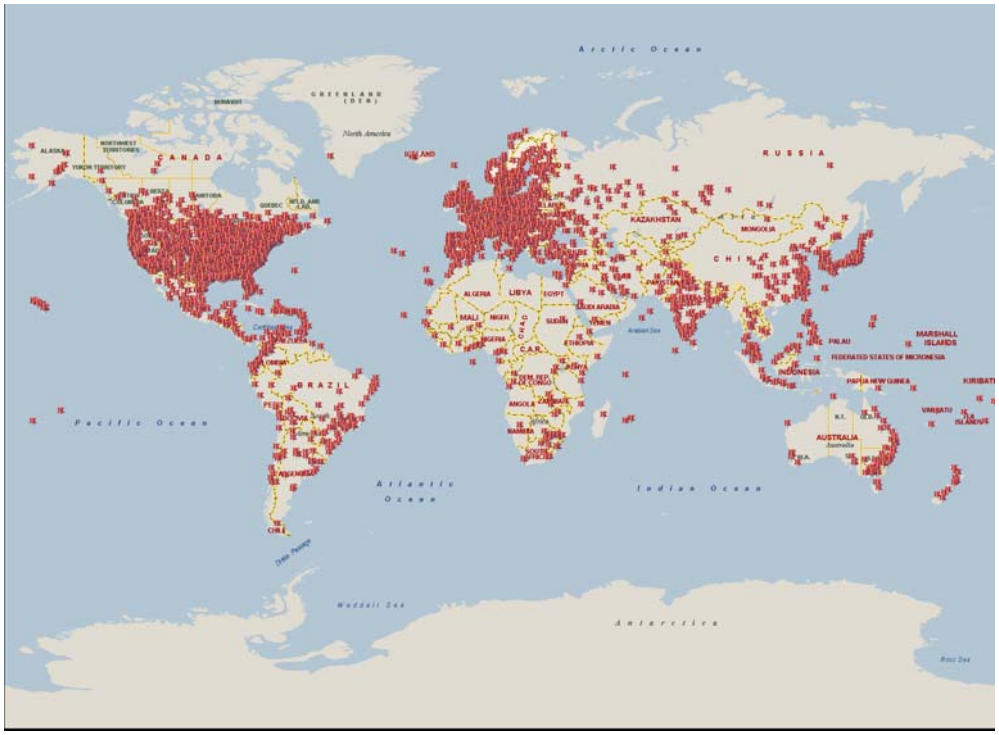
- Se il PC è lento, è vecchio e lo devo cambiare
- I computer MAC sono sicuri (CansecWest – PowOwn) Safari su iPhone, Safari 4 su Mac OSX

Firewall

- Limitare rischi di accesso indesiderato > protezione traffico > ADSL
- Esterno (hardware – network firewall, appliance), Interno (software – Zone Alarm)

Rootkit e Botnet

Rootkit > *(equipaggiamento da Amministratore)* porzione di software
Botnet > *(robot network)* > *Mariposa, Zeus*



IM e CHAT

Instant Message > Svago > Lavoro > one-to-one
Chat Room > many-to-many

Chat Robot > software che interagisce all'interno delle IM e delle Chat
PERICOLI > Identità, vulnerabilità, intercettazioni, configurazioni

P2P (Peer to Peer)

Condivisione > Codice malevolo, esposizione di informazioni, attacchi, malfunzionamenti
Ambiente molto pericoloso perché chi lo frequenta è disposto a rischiare pur di ottenere il file che gli interessa. Per questo è molto frequentato da ogni tipo di malware. Attenti ad aprire i file scaricati senza prima averli testati con un buon AV.

BLUETOOTH

Comunicazione Wireless > Frequenze radio > Autenticazione a chiave > Crittografia > Bluesnarfing

PROTEZIONE

- Disabilitare se non si usa
- Modalità "hidden"
- Ambiente sicuro
- Limitare le abilitazioni
- Sfruttare le sicurezze *(password, PIN)*

SOCIAL NETWORKS

FACEBOOK, FLICKR, TWITTER, WORDPRESS, DELICIOUS, BOGGER, FRIENDFEED
Mettere a disposizione una certa quantità di informazioni personali > attacchi di tipo *"social engineering"*>**PHISHING** *"spillaggio"*
BACKUP > https://secure.backupify.com/signup

RETI WIRELESS

Hotspot > onde radio > wardriving > cambiare password default > Area riservata indirizzi MAC > WEP, WAP. Si lavora in "ambienti aperti" e quindi poco protetti. Attivare le password e le crittografie. Accedere solo a reti conosciute e garantite.

BLINDARE UN COMPUTER

Attacchi per:

- Corrompere > Formattare > Cancellare File
- Spiare
- Rubare informazioni
- Usarci come Zombie

PRIMA COSA: Fare ***Partizioni***, una per il Sistema Operativo (50/60 Gb) ed una per programmi e file personali

SECONDA COSA: Fare ***Copia Immagine*** del PC > ***Drive Image Xml, Ghost.***

L'operazione deve essere fatta quando il PC è ancora nuovo, non ancora "pasticciato" per poter in caso di crash rendere, in tempi ragionevoli, operativa la macchina. Con l'uso di software come quelli suggeriti non occorre essere esperti o guru d'informatica per ripristinare il sistema, bastano poche e semplici operazioni.

PROTEGGERSI DA ATTACCHI DA INTERNET: conoscere IP (Internet Protocol) del vs PC > Shield Up https://www.grc.com/x/ne.dll?bh0bkyd2

- **FILTRO IP** > ***Peerguardian***
- **INTERNET SECURITY SUITE** > ***KASPERSKY, PANDA, NORTON, AVG....***
- **NAVIGARE IN INCOGNITO** > **I2P** (Invisible Intenet Project), **TOR, JONDONYM.**

Il bowser è fondamentale per la tutela della privacy e deve essere configurato correttamente onde evitare di diffondere involontariamente informazioni personali. In IE (Internet Explorer) > Strumenti> Opzioni Internet > Protezione/Privacy.

Io consiglio Firefox, ideale per la navigazione anonima perché sono disponibili molte estensioni interessanti (Adblock Plus, No Script, Quick Local Switcher, Safe Cache, Better Privacy, Cookie Cutter... per citarne alcune). Chi desidera una soluzione già pronta ed efficace può scaricare **"JonDoFox"** (https://anonymous-proxy-server.net/en/jondofox) Installatelo e quando lanciate Firefox potete decidere se utilizzarlo, e navigare al riparo, o usare il Vs solito profilo.

CREARE UN'AREA RISERVATA, VIRTUALIZZARE O.S

Avere un Sistema Operativo "Virtuale" significa avere, all'interno del PC, un'area appunto virtuale, distinta dal reale O.S. e pertanto che possiamo "strapazzare" senza preoccupazione. Quando usciami dall'area virtuale il PC ritorna come prima. In pratica, invece di caricare il sistema operativo, viene caricato un clone che ti permette di eseguire le applicazioni ed eseguire le tue attività online in un ambiente completamente isolato. Il vero sistema operativo non è mai colpito da virus, Trojan, malware e altre minacce. Per tornare al vero sistema operativo è sufficiente riavviare il PC

SOFTWARE> (VirtualBox, VMWare….)

> *Returnil:* è in grado di creare una copia speculare e temporanea del vostro sistema operativo, in memoria RAM o in una parte cache del disco, con cui potete "*sperimentare*" qualsiasi programma, tweak (trucchi per potenziare la performance) che trovate in rete, o navigare in ogni sito, anche il più pericoloso, per scaricare, crackare, anche "beccandovi" un virus.

> *Sandboxie* *(freeware):* ti permette di isolare il O.S. e di lavorare in tranquillità sul tuo computer, effettuando qualunque operazione in un'area protetta ed isolata.

Consente di avviare qualsiasi applicazione installata sul sistema limitandone le possibilità di azione all'interno di un'area protetta, creata appositamente, e denominata "sandbox". L'applicazione (programma) può leggere le informazioni memorizzate in qualsiasi area del sistema ma le operazioni di scrittura, invece, sono ristrette solo ed esclusivamente alla "sandbox".

Utile per fare dei test o per navigare su Internet tutelando la tua privacy.

TENERE SOTTO CONTROLLO PROCESSI > CurrPorts, censire le Porte e sapere quale applicazione o processo le sta interessando e chiuderle.

CRIPTARE LE PARTIZIONI > *TrueCript,* permette di criptare la partizione con il O.S

CONCLUDENDO:

1. Se dovete installare un nuovo programma > "***Returnil***"
2. Installate un programma in una "***SandBoxie***" *e testatelo* prima della sua definitiva installazione
3. Leggete con attenzione i messaggi dei programmi di protezione
4. Quando dovete navigare, attivate "***Returnil***" e aprite il browser in "***SandBoxie***"
5. Prima di inserire una PenDrive attivate "***Returnil***"
6. Navigazione anonima: Firefox.

ANCORA UN CONSIGLIO QUANDO SI USANO PC CON CONDIVISIONE ACCOUNT > "*Windows SteadyState*"

è un tool rilasciato gratuitamente da Microsoft che permette a un amministratore di aule informatiche scolastiche, dove è presente l'accesso a internet, di gestirlo, creando utenti dalla semplice interfaccia e impostando delle restrizioni sia generali sia basate per ogni utente, il blocco dei programmi, la disattivazione di alcune funzioni, la disabilitazione del tasto destro del mouse, la disconnessione automatica dopo un determinato tempo, e tante altre funzioni per proteggere il computer da danni causati da un utente o tutelare la privacy di altre persone che lo utilizzano.
Windows SteadyState è per ora disponibile per sistemi operativi Windows a 32 bit, e può essere scaricato ed installato solo se si ha una copia di Windows XP o Windows Vista originale.
http://www.microsoft.com/italy/windows/products/winfamily/sharedaccess/default.mspx

E ricordate: la sicurezza totale non esiste, questi sono solo alcuni accorgimenti di buon senso per non dover dire parolacce….