Capitolo 10: Sicurezza

IT Essentials 5.0

Traduzione realizzata da:
Maurizio Maggiora
Accademia del Levante – La formazione certificata
m.maggiora@accademiadellevante.org

Cisco | Networking Academy®
Mind Wide Open™

Obiettivi Capitolo 10

- 10.0 Spiegare perché la sicurezza è importante
- 10.1 Descrivere le minacce per la sicurezza
- 10.2 Identificare le procedure di sicurezza
- 10.3 Identificare tecniche comuni di manutenzione preventiva per la sicurezza
- 10.4 Processo di troubleshooting per la sicurezza

L'Importanza della Sicurezza

- Informazioni private, segreti aziendali, dati finanziari, dispositivi informatici e questioni di sicurezza nazionale sono a rischio se non vengono seguite opportune procedure di sicurezza.
- Tra le principali responsabilità di un tecnico vi è la sicurezza dei dati e delle reti.

Minacce alla Sicurezza

Potenziali minacce alla sicurezza del computer:

- Minacce interne
  - I dipendenti possono causare minacce intenzionali o accidentali.
- Minacce esterne
  - Utenti esterni possono effettuare attacchi strutturati o non strutturati.

Tipi di attacchi alla sicurezza del computer:

- Fisica
  - Furto, danneggiamento, distruzione di dispositivi informatici.
- Dati
  - Rimozione, corruzione, negazione dell'accesso, accesso non autorizzato o furto di informazioni.

Adware, Spyware e Phishing

Il **software malevolo (malware)** è un qualunque software progettato per danneggiare o distruggere un sistema:

- **Adware** – programma software che mostra pubblicità sul computer, spesso attraverso una finestra pop-up.
- **Spyware** – distribuito senza l'intervento o la consapevolezza dell'utente, monitora l'attività sul computer.
- **Phishing** – l'aggressore finge di rappresentare un'organizzazione esterna legittima e chiede la verifica di informazioni della vittima, quali nomi utente e password.

Virus, Worm, Trojan e Rootkit

- Un **Virus** è codice software deliberatamente creato da un attaccante. I virus possono raccogliere informazioni sensibili o alterare o distruggere informazioni.
- Un **Worm** è un programma auto-replicante che utilizza la rete per duplicare il proprio codice negli host della rete. Come minimo, i worm consumano banda nella rete.
- Un **Trojan** è un software dannoso travestito da programma legittimo. Il suo nome deriva dal suo modo di oltrepassare le difese del computer facendo finta di essere qualcosa di utile.
- I **software Anti-virus** sono progettati per individuare, disabilitare e rimuovere virus, worm e cavalli di Troia prima che infettino un computer.
- Un **Rootkit** è un programma dannoso che ottiene il pieno accesso a un sistema informatico. Spesso viene usato un attacco diretto sul sistema, sfruttando una vulnerabilità conosciuta o una password nota.

Sicurezza sul Web

Gli strumenti che rendono potenti le pagine web possono rendere il computer vulnerabile:

- **Active X** – Controlla l'interattività nella pagine web.
- **Java** – Consente l'esecuzione di applet all'interno di un browser.
- **Java Script** – Interagisce con il codice sorgente HTML per consentire ai siti web di essere interattivi.
- **Adobe Flash** – Usato per creare media (animazioni, video e giochi) interattivi per il web.
- **Microsoft Silverlight** – Usato per creare media per il web ricchi e interattivi, simile a flash.

La maggior parte dei browser hanno impostazioni per aiutare a prevenire questi attacchi, ad esempio:

- **Filtro ActiveX**
- **Blocco Pop-up**
- **Filtro SmartScreen (Internet Explorer)**

Navigazione in Incognito (InPrivate Browsing)

- La **Navigazione in Incognito (InPrivate Browsing)** impedisce al browser web di memorizzare le seguenti informazioni:
  - Nomi utente
  - Password
  - Cookie
  - Cronologia delle esplorazioni
  - File Temporanei di Internet
  - Dati dei Moduli
- Il browser memorizza i file temporanei e i cookie ma tali informazioni vengono cancellate quando la sessione in Incognito viene terminata.
- Per iniziare la Navigazione in Incognito in Windows 7:
  - Click con il tasto destro del mouse **Internet Explorer > Avvia InPrivate Browsing**

Spam

- Lo **Spam** è un'email non richiesta che può essere usata per inviare link pericolosi o contenuti ingannevoli.
- I **Popup** sono finestre che si aprono automaticamente, progettati per catturare l'attenzione e portare a siti pubblicitari.

Usare software anti-virus, opzioni nel software e-mail, blocco popup e comuni indicatori di spam per combatterli.

Attacchi TCP/IP

La suite TCP/IP controlla la comunicazione su Internet. Può essere manipolata per impedire agli utenti l'accesso ai normali servizi.

- **Denial of Service (DoS)** – invio di abbastanza richieste da sovraccaricare una risorsa o addirittura bloccarne l'operatività.
- **DoS Distribuito (DDoS)** – un attacco lanciato da molti computer, detti **zombie** o **botnet.**
- **SYN Flood** – apre a caso porte TCP alla fonte dell'attacco e impegna con una grande quantità di false richieste SYN il computer.
- **Spoofing** – utilizza un indirizzo IP o MAC falso per impersonare un computer considerato affidabile.
- **Man-in-the-Middle** – intercetta le comunicazioni tra computer per rubare informazioni in trasito attraverso al rete.
- **Replay** – le trasmissioni di dati sono intercettate e registrate da un utente malintenzionato, quindi riprodotte per ottenere l'accesso.
- **DNS Poisoning -** I record DNS sono modificati per indirizzare verso falsi server.

Social Engineering

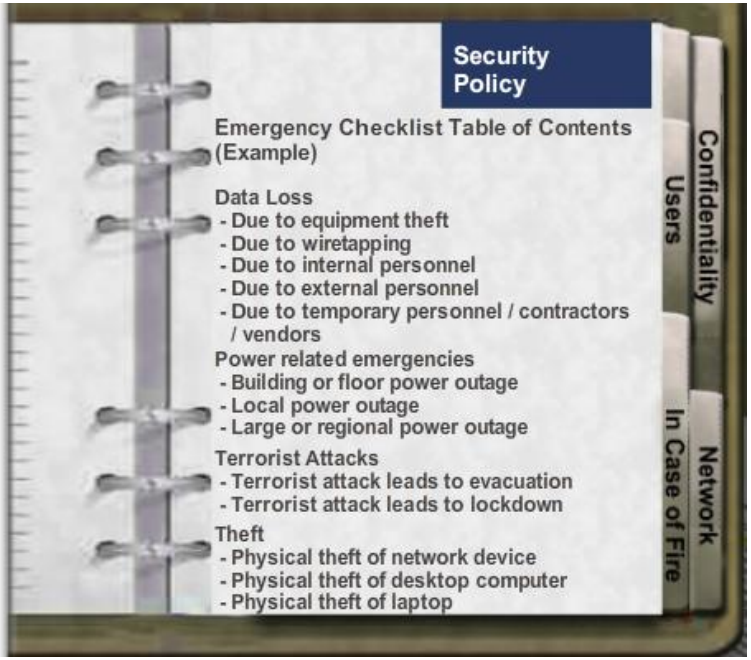
- Un **social engineer** è una persona capace di ottenere l'accesso agli apparati o a una rete inducendo le persone a fornirgli le informazioni necessarie per l'accesso.
- Per proteggersi dal social engineering:
  - Non fornire mai la propria password.
  - Chiedere sempre alle persone sconosciute di identificarsi.
  - Limitare l'accesso ai visitatori.
  - Accompagnare i visitatori.
  - Non affiggere nell'area di lavoro fogli contenenti la password.
  - Bloccare il computer quando ci si allontana dalla scrivania.
  - Non farsi seguire da persone sconosciute quando si passa da una porta che richiede una scheda di accesso.

Distruzione di Hard Disk e Riciclo

- Cancellare tutti gli hard disk, quindi utilizzare uno strumento di data wiping di terze parti per eliminare completamente tutti i dati.
- La smagnetizzazione (degaussing) distrugge o elimina il campo magnetico che consente la memorizzazione dei dati su un hard disk. Uno strumento di smagnetizzazione è molto costoso ed è impraticabile per la maggior parte degli utenti.
- L'unico modo per assicurarsi completamente che i dati non possano essere recuperati da un hard disk è frantumare con attenzione i dischi magnetici con un martello e smaltirne i pezzi in maniera corretta.
- Per distruggere altri supporti di memorizzazione (floppy disk e CD), usare una macchina trituratrice progettata per triturare questi materiali.
- **Riciclo di Hard Disk** – Gli Hard Disk che non contengono dati sensibili possono essere riformattati e usati in altri computer.

Policy di Sicurezza

- Una policy di sicurezza dovrebbe descrivere come un'azienda gestisce i problemi relativi alla sicurezza
- Domande a cui rispondere nella stesura di una security policy locale:
  - Quali risorse richiedono protezione?
  - Quali sono le possibili minacce?
  - Cosa fare nel caso di una violazione della sicurezza?
  - Che tipo di formazione sarà offerta per addestrare gli utenti finali?



Requisiti di una Policy di Sicurezza

Una policy di sicurezza dovrebbe affrontare i seguenti settori chiave:

- Processo per la gestione degli incidenti di sicurezza di rete
- Processo per controllare la sicurezza della rete esistente
- Struttura generale di sicurezza per implementare la sicurezza della rete
- Comportamenti ammessi
- Comportamenti proibiti
- Di cosa creare i log e come archiviarli: Visualizzatore Eventi, file di log di sistema o file di log di sicurezza
- Accesso di rete alle risorse tramite i permessi assegnati a un account
- Tecnologie di autenticazione per accedere ai dati: nomi utente, password, biometria e smart card

Nome utente e Password

Policy per Nome utente e Password:

- Cambiare il nome di default per account quali *administrator* o *guest*.
- L'amministratore di rete definisce una convenzione per determinare i nomi utente.
- Sono consigliati tre livelli di protezione con password:
  - **BIOS**
  - **Login**
  - **Rete**

Requisiti per le Password

Linee guida per la creazione di password robuste:

- **Lunghezza –** Usare almeno 8 caratteri.
- **Complessità –** Includere lettere, numeri, simboli e segni di punteggiatura. Usare una varietà di combinazioni sulla tastiera, non solo lettere e caratteri comuni.
- **Variazione –** Modificare le password frequentemente. Impostare un promemoria per cambiare le password per la posta elettronica, il conto bancario e i siti web delle carte di credito mediamente ogni tre o quattro mesi.
- **Varietà** – Usare una password diversa per ogni sito o computer che si utilizza.

Autorizzazioni per File e Cartelle

- I livelli di autorizzazione sono configurati per limitare l'accesso individuale o di gruppo a dati specifici.
- **NTFS** – File system che usa il journaling, aree speciali dove i cambiamenti ai file sono registrati prima che le modifiche siano eseguite.
  - Può effettuare il log degli accessi per utente, data e ora.
  - Ha capacità crittografiche.
- **FAT32** - nessuna crittografia, né journaling.
- **Principio del Privilegio Minimo** – consentire agli utenti l'accesso alle sole risorse di cui hanno bisogno.
- **Limitazione di Autorizzazioni dell'Utente** – Se a un individuo o ad un gruppo sono negate le autorizzazioni per una condivisione di rete, questa restrizione sostituisce tutte le altre autorizzazioni date.

Protezione dei Dati

Il valore dei dispositivi fisici è spesso molto inferiore al valore dei dati che essi contengono. Ci sono parecchi metodi di protezione di sicurezza che possono essere implementati per proteggere i dati.

- Firewall Software
- Sicurezza con Smart Card
- Sicurezza Biometrica
- Backup dei Dati
- Crittografia dei Dati

Crittografia dei Dati

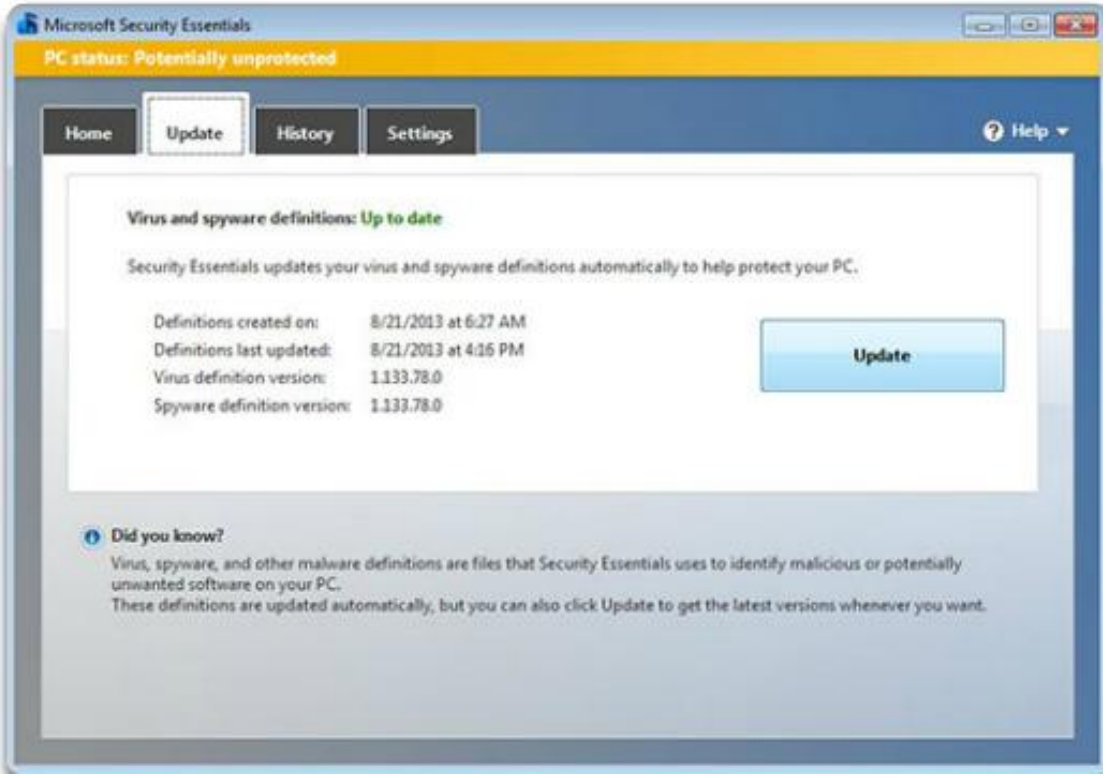
- Crittografia – i dati sono trasformati usando un complicato algoritmo che li rende illeggibili.
- **Encrypting File System (EFS)** è una funzione di Windows in grado di crittografare i dati.
- **BitLocker** può crittografare l'intero volume del disco ed è incluso in Windows 7 e Windows Vista Ultimate e Enterprise edition.
- **Trusted Platform Module (TPM)** è un chip dedicato installato sulla motherboard di un computer da usare per l'autenticazione hardware e software.
  - Il TPM memorizza informazioni specifiche per il sistema host, come ad esempio chiavi di crittografia, certificati digitali e password.

Programmi di Protezione da Software Dannoso

- Il **Malware** è un software dannoso che viene installato su un computer senza la conoscenza o il permesso dell'utente.
- Possono essere necessari diversi programmi anti-malware e numerose scansioni per rimuovere compeltamente tutto il software dannoso.
- Software anti-malware disponibili per questi scopi sono: anti-virus, anti-spyware, anti-adware e programmi anti-phishing.

Aggiornamenti dei File di Firma

- Poiché vengono sempre sviluppati nuovi virus, i software di sicurezza devono essere continuamente aggiornati.



Tipi di Crittografia della Comunicazione

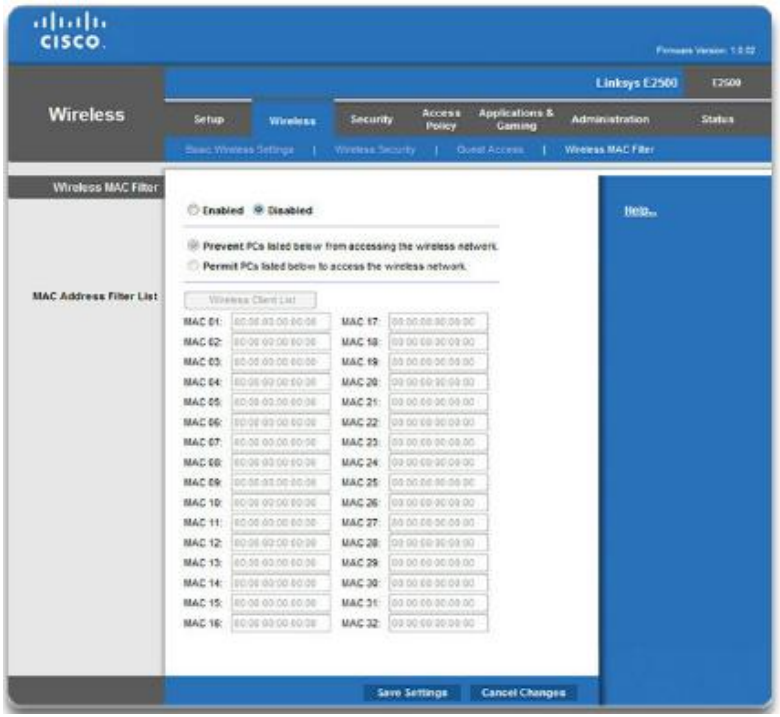
- La **Codifica Hash** usa una funzione matematica per creare un valore numerico univoco per quel particolare dato.
- La **Crittografia Simmetrica** richiede che entrambe le parti di una conversazione criptata usino una chiave di cifratura per codificare e decodificare i dati.
- La **Crittografia Asimmetrica** richiede due chiavi, una chiave privata e una chiave pubblica.

Service Set Identifier

- Il Service Set Identifier (SSID) è il nome della rete wireless. Un router wireless o un access point trasmette di default l'SSID in modo che i dispositivi wireless siano in grado di rilevare la rete wireless.
- Per disattivare la trasmissione dell'SSID, usare il seguente percorso:
- **Wireless > Impostazioni Wireless di Base >** selezionare **Disabilita SSID Broadcast > Salva Impostazioni > Continua**
- Disabilitare la trasmissione dell'SSID fornisce una sicurezza molto limitata. Se la trasmissione dell'SSID è disattivata, ogni utente del computer che desidera collegarsi alla rete wireless deve inserire manualmente l'SSID. Quando un computer è alla ricerca di una rete wireless, trasmetterà l'SSID.

Mac Address Filtering

- Il filtro degli indirizzi MAC è una tecnica usata per implementare la sicurezza a livello di dispositivo su una LAN wireless.



Modalità di Protezione Wireless

- **Wired Equivalent Privacy (WEP)** – La prima generazione di standard di sicurezza per il wireless. Gli attaccanti scoprirono rapidamente che la crittografia WEP era facile da violare.
- **Wi-Fi Protected Access (WPA)** – Versione migliorata del WEP, utilizza una crittografia molto più robusta.
- **Wi-Fi Protected Access 2 (WPA2)** – WPA2 supporta una crittografia robusta, garantendo un grado di sicurezza accettato a livello governativo.

Accesso Wireless

- **Antenne Wireless**
  - Evitare di trasmettere segnali al di fuori dall'area della rete tramite l'installazione di un'antenna con un diagramma di radiazione che serva gli utenti della rete.
- **Accesso al Dispositivo di Rete**
  - Alla prima connessione al dispositivo di rete, cambiare nome utente e password predefiniti.
- **Wi-Fi Protected Setup (WPS)**
  - L'utente si collega al router wireless usando il PIN impostato in fabbrica che è stampato su un adesivo o visualizzato su un display.
  - Sono stati sviluppati software in grado di intercettare il traffico e recuperare il PIN WPS e la chiave di crittografia pre-condivisa. Disabilitare il WPS sul router wireless, se possibile.

Firewall

Firewall Hardware	Software Firewall
Componente hardware dedicato	Disponibile come software di terze parti, il costo varia
Il costo iniziale per aggiornamenti hardware e software può essere oneroso	Versione gratuita inclusa con il sistema operativo Windows
Possono essere protetti più computer	Tipicamente protegge solo il computer su cui è installato
Nessun impatto sulle prestazioni del computer	Utilizza la CPU, potenziale impatto sulle prestazioni del computer

Port Forwarding e Port Triggering

- Il **Port Forwarding** è un metodo basato su regole per dirigere il traffico tra dispositivi su reti separate:
  - Usato quando specifiche porte devono essere aperte affinchè certi programmi e applicazioni possano comunicare con dispositivi su reti diverse.
  - Il router determina se il traffico deve essere inoltrato ad un certo dispositivo sulla base del numero di porta riscontrato nel traffico. Ad esempio, HTTP – Port 80.
- Il **Port Triggering** permette al router di inoltrare temporaneamente i dati attraverso le porte di ingresso verso un dispositivo specifico.
  - Ad esempio, un videogioco potrebbe usare le porte da 27000 a 27100 per il collegamento con gli altri giocatori. Queste sono le porte trigger.

Metodi di Protezione degli Apparati Fisici

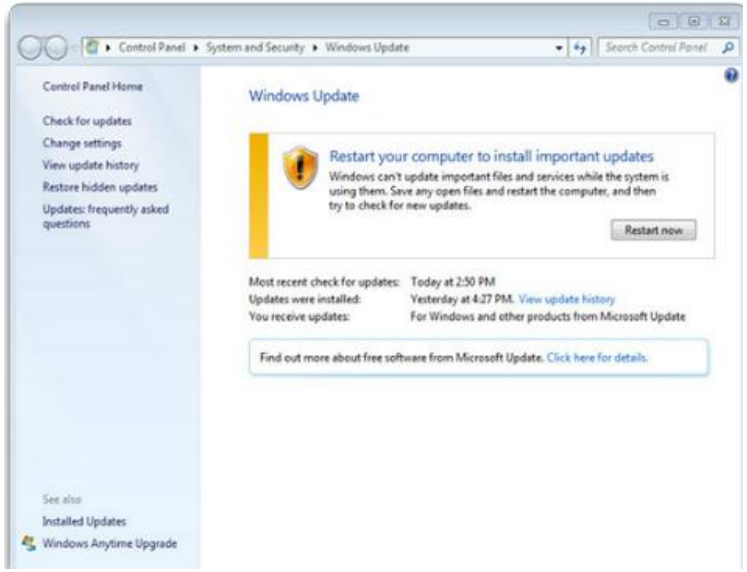
- La sicurezza fisica è importante tanto quanto la sicurezza dei dati. Le infrastrutture di rete possono essere protette da:
  - Messa in sicurezza di locali di telecomunicazioni, armadi per apparati e gabbie di sicurezza.
  - Cavi antifurto e viti di sicurezza per i dispositivi hardware
  - Rilevamento wireless di access point non autorizzati
  - Firewall hardware
  - Sistema di gestione della rete che rileva i cambiamenti nel cablaggio e nei patch panel
- **Autenticazione a due fattori** – messa in sicurezza con tecniche di protezione in sovrapposizione per evitare l'accesso non autorizzato ai dati sensibili.
  - Un esempio di protezione in sovrapposizione consiste nell'usare una password e una smart card per proteggere una risorsa.

Hardware per la Sicurezza

- Ci sono diversi modi per proteggere fisicamente le apparecchiature informatiche:
  - Usare cavi di sicurezza sulle apparecchiature.
  - Mantenere chiusi a chiave i locali delle telecomunicazioni.
  - Adoperare viti di sicurezza per le apparecchiature.
  - Usare gabbie di sicurezza per proteggere le apparecchiature.
  - Etichettare e installare sensori, come le etichette RFID (Radio Frequency Identication), sulle apparecchiature.
  - Installare allarmi fisici attivati da sensori per il rilevamento del movimento.
  - Usare webcam con rilevazione del movimento e software di sorveglianza.
- Per l'accesso alle strutture, vi sono numerose possibilità di protezione:
  - Carte magnetiche che memorizzano i dati dell'utente, compreso il livello di accesso consentito
  - Sensori biometrici che identificano le caratteristiche fisiche degli utenti come le impronte digitali o la retina
  - Postazione con guardia di sicurezza
  - Sensori, quali le etichette RFID, per monitorare le apparecchiature

Service Pack e Patch di Sicurezza

- Aggiornamenti di sicurezza regolari sono essenziali per combattere nuov virus o worm.
- Un tecnico dovrebbe comprendere come e quando installare patch e aggiornamenti.
- Le **Patch** sono aggiornamenti di codice che i produttori forniscono per impedire che un virus o un worm recentemente scoperto possa portare un attacco con successo
- Un **Service Pack** è una combinazione di patch e update.



- Windows scarica e installa automaticamente, per impostazione predefinita, gli aggiornamenti oppure può essere controllato localmente;
- **Start > Tutti i programmi > Windows Update > Cambia impostazioni**

Backup dei Dati

- I backup di Windows possono essere effettuati manualmente o programmati per avvenire automaticamente.
- Per avviare la procedura guidata Backup dei File per la prima volta in Windows 7, usare il seguente percorso:

Start > Tutti i programmi > Manutenzione > Backup e Ripristino> Configura backup

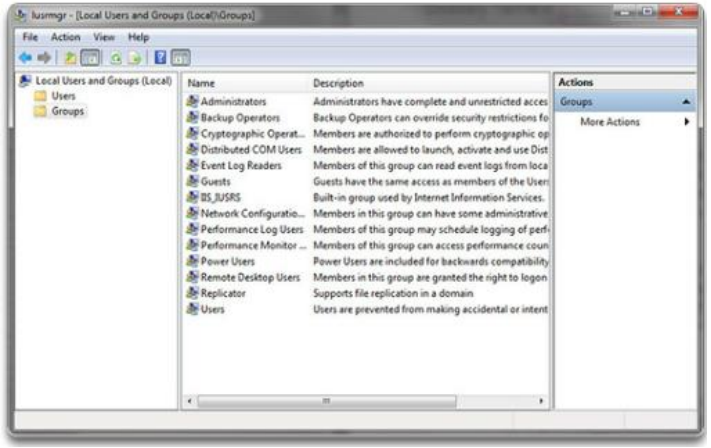
Tipo di backup	Descrizione
Completo o Normale	Questo tipo di backup copia tutti i file selezionati e contrassegna ciascun file che è stato salvato in un backup.
Incrementale	Questo tipo di backup esegue solamente il backup dei file che sono stati creati o modificati dopo l'ultimo backup completo o incrementale. Il ripristino dei file richiede di avere l'ultimo backup completo e tutto il set di backup incrementali.
Differenziale	Questo tipo di backup copia solo i file che sono stati creati o modificati dopo l'ultimo backup completo. Il ripristino dei file richiede che si disponga dell'ultimo backup completo e di un backup differenziale.
Giornaliero	Questo tipo di backup copia tutti i file selezionati che sono stati modificati il giorno in cui il backup giornaliero è stato eseguito.
Copia	Questo tipo di backup copia tutti i file selezionati, ma non li contrassegna come salvati in un backup.

Configurazione di Firewall

- Un **Firewall** impedisce selettivamente i traffico verso un computer o un segmento di rete.
- **Policcy di sicurezza restrittiva** – Un firewall che apre solo le porte richieste. Qualunque pacchetto non esplicitamente permesso, è negato.
- La configurazione del firewall di Windows 7 o Windows Vista può essere completata in due modi:
  - **Automaticamente -** L'utente è invitato a scegliere fra **Continua a Bloccare**, **Sbloccare** o **Richiedi In Seguito** per le richieste non sollecitate.
  - **Gestione Impostazioni di Protezione** – L'utente aggiunge manualmente il programma o le porte che sono richieste dalle applicazioni in uso sulla rete.

Manutenzione degli Account

- Raggruppare i dipendenti in base alle esigenze professionali per avere accesso ai file impostando i permessi di gruppo.
- Quando un dipendente lascia un'organizzazione, l'accesso alla rete deve essere interrotto immediatamente.
- Agli ospiti si può offrire un accesso attraverso un account Guest.
- Per configurare tutti gli utenti e i gruppi su un computer, digitare **lusrmgr.msc** nella casella di ricerca o nella riga di comando dell'utilità Esegui.



Processo di Troubleshooting

Passo 1 Identificare il Problema

Passo 2 Stabilire una Teoria sulle Probabili Cause

Passo 3 Testare la Teoria per Determinare la Causa

Passo 4 Stabilire un Piano d'Azione per la Soluzione del Problema e la Relativa Implementazione

Passo 5 Verificare la Piena Funzionalità del Sistema e Attuare le Misure Preventive

Passo 6 Documentare le Conclusioni, le Azioni e i Risultati

Passo 1 – Identificare il problema

- **Informazioni sul Sistema**
  - Produttore, modello, SO, ambiente di rete, tipo di connessione
- **Domande a Risposta aperta**
  - Quando è iniziato il problema?
  - Che tipo di problema si sta riscontrando?
  - Quali siti web sono stati visitati recentemente?
  - Quale software di sicurezza è installato sul computer?
  - Chi altro ha utilizzato il computer recentemente?
- **Domande a Risposta chiusa (prevedono come risposta sì o no)**
  - Il software di sicurezza è aggiornato?
  - E' stata effettuata di recente la scansione antivirus del computer?
  - E' stato aperto un allegato da un'email sospetta?
  - La password è stata cambiata recentemente?
  - E' stata condivisa la password con qualcuno?

Passo 2 – Stabilire una Teoria sulle Probabili Cause

- Creare una lista delle più comuni cause di problemi di sicurezza:
  - Virus
  - Trojan Horse (Cavallo di Troia)
  - Worm
  - Spyware
  - Adware
  - Grayware o Malware
  - Tecniche di Phishing
  - Password compromessa
  - Locali tecnici non protetti
  - Ambiente di lavoro non sicuro

Passo 3 – Testare la Teoria per Determinare la Causa

- Testare le teorie sulle probabili cause una alla volta, cominciando con la più veloce e semplice.
  - Scollegarsi dalla rete
  - Aggiornare le definizioni dell'antivirus e dell'antispyware
  - Effettuare una scansione del computer tramite il software di protezione
  - Controllare che il SO del computer contenga gli ultimi aggiornamenti e patch
  - Riavviare il computer o il dispositivo di rete
  - Accedere con un utente diverso e cambiare la propria password
  - Mettere in sicurezza i locali tecnici
  - Mettere in sicurezza l'ambiente di lavoro
  - Applicare le policy di sicurezza
- Se la causa esatta del problema non è stata determinata dopo che tutte le teorie sono state testate, stabilire una nuova teoria di cause probabili e testarla.

Passo 4 – Stabilire un Piano d'Azione per la Soluzione del Problema e la Relativa Implementazione

- Dopo aver determinato la causa esatta del problema, stabilire un piano d'azione per risolvere il guasto e implementare la soluzione.
- Talvolta procedure veloci possono determinare la causa esatta del problema o addirittura correggere il guasto.
- Se una procedura veloce non risolve il problema, potrebbe essere necessario effettuare ulteriori richerche sul guasto per stabilire la causa esatta

Passo 5 – Verificare la Piena Funzionalità del Sistema e Attuare le Misure Preventive

- Verificare la piena funzionalità del sistema e, se necessario, attuare misure di prevenzione.
  - Effettuare una nuova scansione del computer per verificare che non siano rimasti virus.
  - Effettuare una nuova scansione del computer per verificare che non siano rimasti spyware.
  - Controllare i log del software di sicurezza per verificare che non vi siano problemi residui.
  - Controllare che il SO del computer contenga gli ultimi aggiornamenti e patch.
  - Verificare la connettività di rete e Internet.
  - Assicurarsi che tutte le applicazioni siano funzionanti.
  - Verificare l'accesso a risorse autorizzate quali stampanti condivise e database.
  - Assicurarsi che gli accessi siano sicuri.
  - Assicurarsi che la politica di sicurezza venga applicata.
- Assicurarsi che il cliente verifichi la soluzione e la funzionalità del sistema.

Passo 6 – Documentare le Conclusioni, le Azioni e i Risultati

- Discutere la soluzione con il cliente
- Far verificare al cliente che il problema è stato risolto.
- Documentare il processo:
  - Descrizione del problema
  - Soluzione
  - Componenti usati
  - Tempo impiegato per risolvere il problema

Problemi Comuni e Soluzioni

- Fare riferimento alla tabella nel curriculum per Problemi Comuni e Soluzioni per la Sicurezza

Riepilogo Capitolo 10

- Seguire corrette procedure di sicurezza protegge i computer e gli apparati di rete e i dati che essi contengono da danni fisici, quali incendi e furti, e da perdite e danneggiamenti da parte di dipendenti e attaccanti.
- Le minacce alla sicurezza possono provenire dall'interno o dall'esterno di un'organizzazione.
- I virus e i worm sono minacce comuni che attaccano i dati.
- Sviluppare e mantenere un piano di sicurezza come protezione da perdita di dati e danni agli apparati.
- Mantenere aggiornati e sicuri i sistemi operativi e le applicazioni con le patch e i service pack.