

Dispensa di Sicurezza Informatica (Parte 2)

CAPITOLO 4 – CONTROLLI DEGLI ACCESSI

- **Identificare i Metodi per Impedire Accessi non Autorizzati ai Dati**
 - L'obiettivo principale dei controlli degli accessi è impedire che persone non autorizzate accedano ai dati.
 - I metodi includono l'uso di nome utente, password, PIN, impronta digitale o altre tecniche di autenticazione.
- **Autenticazione**
 - È il processo tramite il quale un sistema informatico **verifica l'identità** di un utente che cerca di accedere alle sue risorse.
 - In pratica, un utente autorizzato deve dimostrare la propria identità prima di poter utilizzare le risorse.
 - L'autenticazione si basa tipicamente su una combinazione di fattori che l'utente deve fornire o possedere:
 - **Qualcosa che si conosce:** Come una **password** o un **PIN**.
 - **Qualcosa che si possiede:** Come un passaporto digitale, una smart card.
 - **Qualcosa che si è:** Come un'impronta digitale, la voce, la retina o altri **identificatori biometrici**.
 - L'autenticazione può essere semplice (basata su un singolo fattore) o più **robusta/forte** (combinando più fattori). L'autenticazione forte si verifica quando si usano più metodi per accedere a una funzionalità o servizio.
- **Crittografia nel Processo di Autenticazione**
 - Quando l'autenticazione non coinvolge direttamente un essere umano (es. trasmissione dati), la crittografia gioca un ruolo fondamentale.
- **Comprendere il Termine "One-Time Password" (OTP)**
 - Una **password usa e getta** che può essere utilizzata solo una volta, per una singola sessione o transazione.
 - Le OTP risolvono i problemi legati all'uso di password tradizionali e offrono protezione contro gli attacchi di "replay" (riutilizzo di credenziali intercettate).
 - Un intruso che intercetta un'OTP già utilizzata non potrà riutilizzarla per accedere al servizio.
 - Le OTP possono essere generate in vari modi: chiavette con display, software su smartphone (molto usato nel **home banking**), SMS, o liste stampate in possesso dell'utente.
- **Comprendere lo Scopo di un Account di Rete**

- In una rete di computer, l'autenticazione degli utenti è necessaria per distinguere tra **parti (client) e server**.
- I client si affidano ai server per l'accesso a risorse condivise.
- Nelle organizzazioni aziendali basate su un **dominio**, i client/server sono gestiti centralmente da un server.
- Un account di rete, gestito a livello di dominio, è diverso da un account locale sul singolo computer. Permette all'utente di effettuare il login su qualsiasi computer del dominio usando le stesse credenziali.
- L'account di rete (composto da **nome utente e password**) identifica l'utente e viene utilizzato per regolare il suo accesso alle risorse di rete (file, stampanti, ecc.). Queste regole sono definite dall'**Access Control List (ACL)** gestita dall'amministratore di rete.
- **Accesso alla Rete con Nome Utente e Password e Blocco dell'Account**
 - Per accedere alle risorse di rete, l'utente deve autenticarsi con il proprio nome utente e password.
 - L'accesso avviene tipicamente dopo il login iniziale.
 - Dopo il login, si ha accesso al proprio profilo locale e alle risorse condivise autorizzate.
 - È importante **bloccare lo schermo** del PC quando ci si allontana temporaneamente. Questo impedisce ad altri di usare il computer mantenendo la sessione utente attiva.
 - Lo schermo può essere bloccato manualmente o automaticamente.
 - Se il PC deve essere usato da altri, è necessario eseguire la **disconnessione (logout)** o lo spegnimento per garantire che il prossimo utente acceda con il proprio account. Su Windows 7, bloccare la sessione non chiude i programmi in esecuzione ma richiede l'autenticazione per riaccedere.
- **Identificare le Comuni Tecniche di Sicurezza Biometriche**
 - Le tecniche biometriche si basano sulla scansione di una **caratteristica fisica umana unica** per l'identificazione.
 - Sono più diffuse sui dispositivi mobili che sui computer tradizionali.
 - Esempi comuni:
 - **Scansione dell'impronta digitale:** Basata sull'analisi delle creste e valli dei polpastrelli.
 - **Riconoscimento facciale:** Analisi della geometria del volto (occhi, naso, bocca, ecc.).
 - **Scansione dell'iride/retina:** Analisi dei pattern nell'occhio.
 - **Riconoscimento della voce:** Analisi delle caratteristiche vocali.
 - **Geometria della mano:** Basata su forma e dimensioni della mano.
- **Riconoscere Buone Linee di Condotta per la Password**
 - Una password robusta è fondamentale per la sicurezza.
 - Linee guida per una password sicura:

- Deve essere **segreta** e non scritta.
 - Verificare regolarmente se è stata compromessa.
 - Deve avere una **lunghezza adeguata** (almeno 8 caratteri consigliati, combinando lettere, numeri e simboli).
 - Deve essere **robusta/complessa**.
 - Non deve essere facilmente riconducibile all'utente (nome, data di nascita, ecc.) o una parola di dizionario.
 - È consigliabile utilizzare **password diverse** per servizi diversi.
- Attenzione: Usare una password troppo complessa su tastiere o sistemi operativi diversi può causare problemi di digitazione.
- **Comprendere la Funzione e le Limitazioni dei Software di Gestione delle Password**
 - La crescente quantità di siti che richiedono password rende difficile ricordarne molte, diverse e complesse. Molti utenti tendono a usare la stessa password o password deboli.
 - Una soluzione è l'uso di un **Password Manager**.
 - È un software specializzato per **conservare le password in modo sicuro**, solitamente cifrate.
 - Richiede all'utente di ricordare una sola password, la "**Master Password**", che deve essere robusta.
 - Il programma si occupa di compilare automaticamente i campi di login e può aiutare a generare password complesse.
 - Esistono diverse tipologie (integrate nei browser, desktop, online/a pagamento). Le versioni online/desktop offrono funzionalità aggiuntive come la creazione di password casuali. Le versioni online permettono l'accesso alle password da diversi dispositivi.

CAPITOLO 5 – USO SICURO DEL WEB

- **Usare un Browser Sicuro e Eliminare i Dati Privati**
 - È importante configurare il browser per un uso sicuro.
 - Disabilitare funzionalità come il **completamento automatico** e il **salvataggio automatico delle password** quando si compilano moduli web. Sebbene comodi, questi strumenti possono rappresentare un rischio per la privacy, specialmente su computer condivisi.
 - **Eliminare i dati privati** memorizzati dal browser, come cronologia di navigazione, cookie, password salvate e file temporanei internet. Questo può essere fatto per liberare spazio o per mantenere la privacy.
 - La navigazione "InPrivate" (o equivalente) consente di non memorizzare la cronologia della sessione corrente.
- **Utilizzare una Connessione di Rete Sicura per le Attività Sensibili**
 - La navigazione web ordinaria presenta rischi limitati.

- Attività che coinvolgono dati sensibili, come acquisti online o operazioni bancarie, richiedono maggiore attenzione alla sicurezza.
- Il protocollo **HTTP** (Hypertext Transfer Protocol) trasmette i dati **in chiaro**, rendendoli vulnerabili all'intercettazione.
- Il protocollo **HTTPS** (Hypertext Transfer Protocol Secure) utilizza la crittografia (SSL/TLS) per rendere la comunicazione tra browser e sito web **sicura**. È indicato dall'indirizzo che inizia con "https://" e dall'icona di un **lucchetto** nella barra degli indirizzi del browser.
- L'uso di HTTPS e la presenza del lucchetto sono indicatori che i dati trasmessi sono cifrati e il sito è autenticato tramite un **certificato digitale**.
- **Identificare le Modalità con Cui Confermare l'Autenticità di un Sito Web**
 - Il crimine informatico e il **phishing** (creazione di siti web fasulli per carpire dati) sono minacce in crescita.
 - Per valutare l'affidabilità di un sito, considerare la qualità dei contenuti (evitare errori grammaticali, offerte irreali).
 - Verificare la presenza di informazioni di contatto valide (telefono, indirizzo, P.IVA).
 - Controllare il **nome del dominio**.
 - Per transazioni sicure, verificare la presenza di HTTPS, lucchetto e dettagli del certificato digitale.
 - Strumenti di verifica online come i tool Whois possono fornire informazioni sul registrante del dominio e sulla data di creazione del sito.
- **Comprendere il Termine "Pharming"**
 - Il pharming è una tecnica di attacco simile al phishing che mira a reindirizzare l'utente da un sito web legittimo a uno **fasullo**.
 - Questo può avvenire modificando la configurazione DNS o il file hosts del computer dell'utente.
 - L'utente potrebbe non accorgersi del reindirizzamento, specialmente se non controlla attentamente l'indirizzo nella barra del browser o il certificato digitale.
- **Comprendere la Funzione e i Tipi di Software per il Controllo del Contenuto**
 - Sono software utilizzati per **filtrare i contenuti** a cui si può accedere tramite internet.
 - Sono usati per impedire l'accesso a materiale inappropriato, bloccare tipi specifici di download (musica, video, programmi) o limitare l'accesso a specifiche risorse di rete.
 - Contribuiscono a migliorare la sicurezza riducendo l'esposizione a potenziali minacce e l'utilizzo improprio della banda di rete.
 - Sono spesso inclusi nei software di "Controllo genitoriale".

