

5 I RISCHI PER LE AZIENDE

In questa lezione vedremo:

- ▶ L'estrema importanza che rivestono le linee guida e politiche per l'uso delle ICT
- ▶ L'importanza della protezione delle informazioni commerciali e finanziarie
- ▶ Le minacce ai dati, interne e esterne
- ▶ L'ingegneria sociale e i suoi metodi
- ▶ Le reti, la loro gestione e messa in sicurezza
- ▶ Il ruolo dell'amministratore
- ▶ Alcuni strumenti tecnici di protezione e le procedure di salvataggio e ripristino dei dati



Le minacce ai dati aziendali

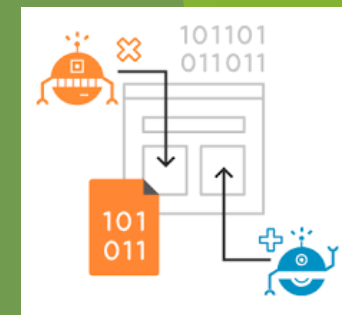
2/3

► Linee guida e politiche per l'uso dell'ICT

Il documento che formalizza tali politiche e linee guida deve essere comunicato al personale in modo che tutti gli addetti conoscano la posizione dell'azienda sui vari aspetti legati all'uso del sistema informativo e delle risorse informatiche e possano attenersi alle regole aziendali destinate ad assicurare una corretta gestione delle ICT

► L'ingegneria sociale e le sue applicazioni

L'ingegneria sociale si basa sui rapporti umani, più che sulla conoscenza di tecniche avanzate, e sulla psicologia delle persone, più che su strumenti tecnologici, con scopi fraudolenti quali carpire informazioni personali o riservate, ottenere credenziali di autenticazione per accedere a sistemi informatici, compiere furti di dati o di identità per sostituirsi ad altri per compiere frodi, malversazioni o reati



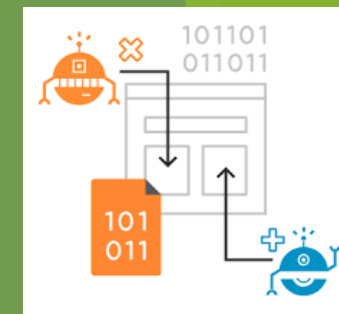
Le minacce ai dati aziendali

3/3

Riconoscere le minacce ai dati provocate da circostanze straordinarie

Molte imprese, soprattutto quelle di una certa dimensione o quelle che trattano dati dei clienti di particolare importanza (si pensi alle banche e alle assicurazioni, ai grandi ISP), mettono in atto delle vere e proprie politiche di **disaster recovery** che garantiscono una ripartenza del sistema informatico in tempi ridotti, anche in caso di distruzione totale provocate da cause di forza maggiore (**catastrofi naturali, eventi straordinari, ecc.**), magari in luoghi diversi rispetto alla loro sede originaria.

- ▶ Nessuno può impedire il verificarsi di calamità naturali. **Terremoti, tempeste, inondazioni, fulmini e incendi** possono causare danni gravi ai computer, che possono risultare in perdita di informazioni, tempi di inattività o perdite di produttività. I danni all'hardware possono inoltre danneggiare altri servizi essenziali
- ▶ Le difese che è possibile predisporre contro le calamità naturali non sono molte. L'approccio migliore consiste nel preparare in anticipo dei piani di ripristino e di emergenza
- ▶ In questa categoria rientrano anche minacce quali **sommosse, guerre e attacchi terroristici** che pur avendo origine umana sono classificate come calamità



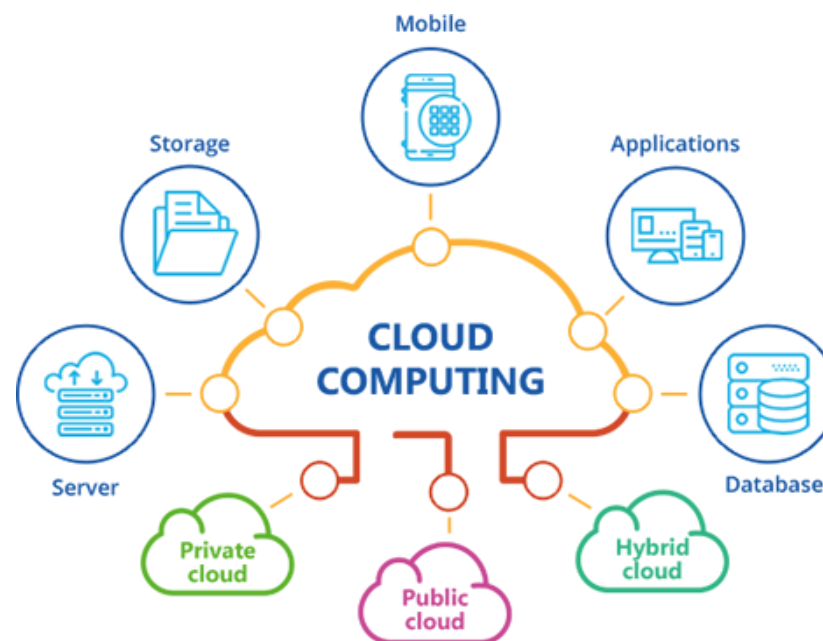
Le minacce ai dati provocate dal cloud computing

Il cloud computing è il recente trend nel mondo IT che ha permesso di spostare l'elaborazione e la memorizzazione dei dati dai PC aziendali alle grandi server farm remote utilizzando la rete Internet.

Innanzitutto aderendo ad un contratto di cloud computing si perde il controllo sui dati fisici, dato che è quasi impossibile stabilire dove siano realmente immagazzinati.

Inoltre, la memorizzazione di dati sensibili espone l'utente a potenziali problemi di violazione della privacy. Un provider scorretto potrebbe accedere ai dati personali e condurre ricerche di mercato o catalogare gli utenti.

Naturalmente, in questo contesto la crittografia può essere d'aiuto

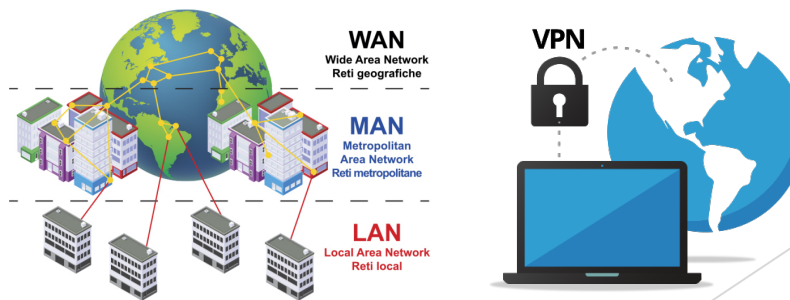


I più comuni tipi di rete

Una rete può essere definita come un insieme di computer (ed eventualmente di altri dispositivi elettronici) collegati fra di loro in modo da consentire la condivisione di risorse comuni (spazio di archiviazione, archivi, stampanti, ecc.) nonché lo scambio di informazioni da parte degli utenti con vari sistemi di comunicazione. Insieme al concetto di rete è l'insieme delle procedure di sicurezza che garantisce l'accesso ai dati soltanto agli utenti autorizzati. Utenti che dispongono di credenziali di autenticazioni (codice utente e password per esempio) per farsi riconoscere e che accedono ai servizi offerti dalle rete limitatamente ai diritti di cui dispongono nel sistema.

Si identificano pertanto tre tipi di reti, a seconda della loro estensione:

- ▶ LAN (Local Area Network), fra le quali troviamo le WLAN (Wireless Local Area Network)
- ▶ MAN (Metropolitan Area Network)
- ▶ WAN (Wide Area Network)
- ▶ VPN (Virtual Private Network)



Come accedere alla rete con le credenziali

Nome utente e password costituiscono le principali credenziali di autenticazione per l'accesso ad un sistema di elaborazione. Ogni utente all'interno dell'impresa o dell'organizzazione sarà dotato di un account personale di rete al quale sarà abbinato un codice utente e una password, quest'ultima da scegliere nel rispetto delle regole aziendali e da modificare periodicamente. Si ricorda infatti che la funzione del nome utente e della password nell'account di rete è duplice:

- ▶ **Autenticazione:** per identificare chi si collega e permettere il collegamento solo a chi è in possesso delle credenziali
- ▶ **Autorizzazione:** all'account di rete sono associati i diritti di accesso alle risorse, configurati in modo che ogni utente possa accedere soltanto alle risorse informatiche di cui necessita nell'ambito della sua attività



Il ruolo dell'amministratore di rete

L'amministratore di rete è la persona interna o esterna all'azienda o all'organizzazione. Assume un ruolo particolarmente importante sulle tematiche di sicurezza ed in particolare deve:

- ▶ Assicurare il regolare funzionamento delle apparecchiature di rete e dei dispositivi di collegamento
- ▶ Definire e mettere in opera le misure di sicurezza atte a garantire un corretto livello di protezione della rete
- ▶ Gestire tutti gli aspetti dell'accesso alla rete da parte degli utenti



Su quest'ultimo punto in particolare, deve:

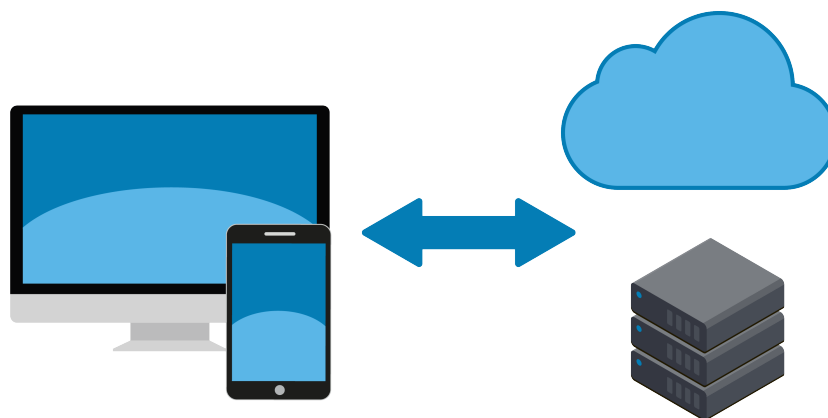
- ▶ Creare gli account utente e assegnare le credenziali di autenticazione (codice utente e password) ai nuovi utenti
- ▶ Assegnare le autorizzazioni ai nuovi utenti (diritti di accedere ad alcuni dati o programmi e non ad altri, a seconda delle mansioni svolte)
- ▶ Aggiornare le autorizzazioni degli utenti (per esempio, in caso di cambio di mansioni che portano a gestire dati diversi)
- ▶ Rimuovere gli account degli utenti che lasciano la struttura

La procedura di copie

Quello della pianificazione e gestione dei backup è un tema molto importante per le imprese, vuoi per la natura dei dati che gestiscono, vuoi per il maggior numero di attacchi che possono ricevere, vuoi ancora per i rischi provenienti dall'interno.

Vediamo ora una cosa molto importante, Per essere affidabile, una procedura di copie di sicurezza deve definire diverse caratteristiche quali:

- ▶ Regolarità
- ▶ Frequenza
- ▶ Pianificazione
- ▶ Collocazione



La funzione del firewall

Più in dettaglio, il compiti del firewall sono:

- ▶ Impedire l'accesso ad Internet di applicazioni presenti sul computer che non sono abilitate ad accedere all'esterno
- ▶ Impedire l'accesso alla rete interna da parte di applicazioni esterne che non sono abilitate ad accedere all'interno della rete o del computer
- ▶ Filtrare contenuti non adatti al contesto di utilizzo
- ▶ Segnalare all'utente e all'amministratore di rete i tentativi di accesso non autorizzati



Comprendere il termine “autorizzazioni dell’applicazione”

- ▶ Ogni app che viene installata, per poter funzionare richiede delle autorizzazioni: una sorta di badge nel quale sono indicate quali risorse del dispositivo potrà utilizzare
- ▶ La visualizzazione di queste richieste prima dell’installazione ha lo scopo di impedire la diffusione di app dannose in quanto le app necessitano di queste autorizzazioni per poter eseguire quello per cui sono state create



Le applicazioni mobili

Queste app possono estrarre informazioni private dal dispositivo mobile.

L'elenco delle autorizzazioni richieste dalle app è molto variegato e comprende termini di non chiara e immediata comprensione.

- ▶ In buona sostanza è bene sapere che le app possono accedere a molte informazioni di carattere personale quali: contatti, cronologia di navigazione, segnalibri, localizzazione GPS, foto e video
- ▶ È quindi opportuno verificare se l'applicazione che si sta utilizzando utilizza autorizzazioni coerenti con il proprio scopo, oppure no, e quindi regolarci di conseguenza

