SECONDA PARTE

1) *In relazione al tema proposto nella prima parte, il giornale offre servizi autenticati di consultazione. Il candidato spieghi il funzionamento dei protocolli https e ssl e gli strumenti di cui è necessario dotarsi per la loro implementazione.*

I protocolli HTTPS (HTTP Secure) e SSL (Secure Sockets Layer) sono utilizzati per garantire la sicurezza delle comunicazioni su Internet e proteggere i dati sensibili degli utenti durante il trasferimento tra il browser e il server web.
Il funzionamento di HTTPS e SSL si basa sull'utilizzo di certificati digitali, chiamati anche certificati SSL/TLS, che vengono emessi da una Certification Authority (CA) e utilizzati per autenticare il server web e criptare i dati scambiati tra il browser e il server.
Così facendo, la connessione è resa sicura e i dati trasmessi sono protetti da possibili attacchi informatici.
Per implementare correttamente i protocolli HTTPS e SSL, è necessario dotarsi di alcuni strumenti e procedure:

Certificato SSL: è necessario acquistare un certificato SSL da una CA affidabile e installarlo sul server web. Questo certificato serve per autenticare il server e criptare le comunicazioni.

Configurazione del server web: è importante configurare correttamente il server web per supportare HTTPS e SSL. Questo può variare a seconda del tipo di server utilizzato (Apache, Nginx, IIS, etc.).

Aggiornamento dei link e delle risorse: è necessario aggiornare tutti i link e le risorse presenti sul sito web per utilizzare il protocollo HTTPS anziché HTTP. È importante che tutte le risorse vengano servite in modo sicuro per evitare eventuali errori di sicurezza.

Monitoraggio e gestione dei certificati: è importante monitorare lo stato dei certificati SSL e rinnovarli prima della loro scadenza per evitare interruzioni nei propri servizi.

Implementare correttamente HTTPS e SSL è fondamentale per garantire la sicurezza delle comunicazioni su Internet e proteggere i dati sensibili degli utenti. È importante seguire le best practice e utilizzare strumenti adeguati per assicurarsi che la connessione sia sicura e affidabile.

2) *In relazione al tema proposto nella prima parte, si discuta della necessità di offrire ad alcuni giornalisti della redazione la possibilità di lavorare da casa, esponendo le tecniche utilizzate ed i protocolli di sicurezza necessari.*

Lavorare da casa come giornalista può essere un'opzione vantaggiosa per diversi motivi, tra cui la flessibilità di orari, la possibilità di evitare gli spostamenti e garantire maggiore concentrazione sul lavoro. Tuttavia, è fondamentale garantire la sicurezza dei dati sensibili della redazione durante questo processo.

Una delle tecniche più utilizzate per consentire ai giornalisti di lavorare da casa in modo sicuro è l'utilizzo di una Virtual Private Network (VPN) di tipo remote access, essa permette agli utenti di connettersi alla rete aziendale in modo sicuro da remoto, crittografando la connessione e proteggendo i dati da potenziali attacchi esterni.

Per implementare una VPN di tipo remote access, è necessario seguire alcuni protocolli di sicurezza.
In primo luogo, è essenziale che sia impostato un forte sistema di autenticazione per garantire che solo gli utenti autorizzati possano accedere alla rete aziendale. Inoltre, è importante aggiornare regolarmente il software della VPN (ad esempio Open VPN) per coprire eventuali vulnerabilità di sicurezza.

Per garantire un accesso sicuro e controllato alla rete aziendale, è possibile utilizzare un server AAA (Authentication, Authorization, and Accounting). Questo server controlla l'accesso degli utenti alla rete, verificando le credenziali di autenticazione, autorizzando gli utenti ad accedere a determinate risorse e monitorando le attività dell'utente per garantire la conformità alle normative di sicurezza.

Inoltre, è consigliabile utilizzare un firewall per controllare il traffico in entrata e in uscita dai dispositivi dei giornalisti che lavorano da casa. In questo modo è possibile monitorare e bloccare eventuali minacce provenienti dall'esterno.

Infine, è importante sensibilizzare i giornalisti sull'importanza di seguire le best practice di sicurezza informatica, come evitare di condividere password o dati sensibili tramite email non criptate e utilizzare solo reti Wi-Fi sicure per connettersi alla VPN.

In conclusione, l'offerta della possibilità di lavorare da casa ai giornalisti della redazione può essere vantaggiosa, ma è essenziale implementare le giuste misure di sicurezza, come una VPN di tipo remote access, per proteggere i dati sensibili della redazione da potenziali minacce esterne.

3) *I documenti, anche importanti, viaggiano sempre più spesso in rete ponendo in evidenza la necessità di garantire sia l'integrità degli stessi che l'identità del mittente. Descrivere la tecnica che garantisce quanto sopra, anche avvalendosi di schemi.*

Una delle tecniche più comuni per garantire l'integrità dei documenti e l'identità del mittente è l'utilizzo della crittografia a chiave pubblica e privata.

In questa tecnica, ogni individuo dispone di una coppia di chiavi: una chiave privata e una chiave pubblica. La chiave privata è conosciuta solo dal mittente e viene utilizzata per firmare digitalmente un documento, garantendo così l'autenticità dell'origine e l'integrità del contenuto. La chiave pubblica, invece, è resa nota a tutti e può essere utilizzata da chiunque per verificare la firma digitale del mittente.

Il processo di firma digitale avviene in due fasi. Innanzitutto, il mittente calcola l'hash del documento usando un algoritmo di hash crittografico.
Successivamente, utilizza la propria chiave privata per crittografare l'hash, generando così la firma digitale.

Il destinatario riceve il documento firmato digitalmente insieme alla chiave pubblica del mittente. Per verificare l'autenticità del documento, il destinatario calcola l'hash del documento ricevuto e utilizza la chiave pubblica del mittente per decriptare la firma digitale e ottenere l'hash originale.

Se i due hash coincidono, il documento è stato verificato con successo.

Questa tecnica garantisce che il documento non sia stato modificato durante il trasferimento e che provenga effettivamente dal mittente che afferma di averlo inviato. Inoltre, la coppia di chiavi rende impossibile a terzi falsificare la firma digitale, garantendo quindi la sicurezza e l'integrità delle comunicazioni online.

4) *La rete, oltre alla posta elettronica, offre agli utenti numerosi servizi quali FTP, DNS, pagine web, ecc., che possono essere di tipo connesso o non connesso. Si descrivano le caratteristiche dei servizi connessi e non connessi riferendosi ad esempi concreti.*

I servizi connessi sono quelli che richiedono una connessione costante tra il client e il server per poter trasmettere informazioni in entrambe le direzioni, in questo caso, è necessario stabilire una sessione di comunicazione prima di poter scambiare dati.

Un esempio di servizio connesso è il trasferimento di file tramite FTP (File Transfer Protocol), dove il client deve autenticarsi presso il server e stabilire una connessione prima di poter inviare o ricevere file.

I servizi non connessi, invece, non richiedono una connessione costante e i dati possono essere trasmessi in modo indipendente l'uno dall'altro.
Un esempio di servizio non connesso è il DNS (Domain Name System), che traduce i nomi di dominio in indirizzi IP senza la necessità di una connessione persistente tra client e server.
Altri esempi di servizi non connessi includono la navigazione web e la posta elettronica.

In generale, i servizi connessi sono più adatti per trasferire grandi quantità di dati in modo affidabile e sicuro, mentre i servizi non connessi sono più adatti per trasmettere informazioni in modo rapido e efficiente senza la necessità di una connessione permanente.