Quali sono i protocolli di sicurezza informatica più comuni?

Maria Cattini | 05/05/2025 | Sicurezza digitale

La sicurezza informatica è una delle principali preoccupazioni nel mondo digitale di oggi. Con l'aumento delle minacce online, proteggere i dati sensibili, le comunicazioni e i sistemi aziendali è diventato fondamentale. I **protocolli di sicurezza informatica** giocano un ruolo cruciale in questo processo, poiché definiscono le regole e le pratiche necessarie per garantire che le informazioni siano protette durante la trasmissione e l'archiviazione.

In questo articolo esploreremo i protocolli di sicurezza informatica più comuni e come contribuiscono a garantire la sicurezza nel cyberspazio. Tra questi, alcuni sono utilizzati per proteggere le comunicazioni, altri per gestire l'accesso a risorse sensibili, e altri ancora per difendere i sistemi contro attacchi esterni.

Cosa sono i protocolli di sicurezza informatica?

Un **protocollo di sicurezza informatica** è una serie di regole e linee guida che stabiliscono come proteggere i dati e le comunicazioni all'interno di una rete o tra dispositivi. Questi protocolli si occupano di gestire aspetti cruciali come la **confidenzialità**, **l'integrità** e la **disponibilità** delle informazioni, nonché la **autenticazione** e la **verifica dell'identità** degli utenti. Ogni protocollo ha uno scopo specifico e viene scelto in base al tipo di comunicazione o interazione che si vuole proteggere.

I protocolli di sicurezza più comuni

1. HTTPS (HyperText Transfer Protocol Secure)

Il **HTTPS** è il protocollo di sicurezza utilizzato per garantire la **sicurezza delle comunicazioni su Internet**. È una versione sicura dell'HTTP, che aggiunge uno strato di crittografia grazie all'uso del **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**.

• Cosa fa: HTTPS cifra i dati scambiati tra il browser dell'utente e il server, impedendo che terze parti possano intercettare, leggere o manipolare le informazioni. Questo è particolarmente importante durante le transazioni bancarie online, l'inserimento di credenziali o l'acquisto di beni.
• Quando viene utilizzato: Ogni volta che si inseriscono informazioni sensibili su un sito web, come login, password o dati di pagamento.

Pro: Garantisce la protezione contro l'intercettazione delle comunicazioni. **Contro**: Richiede una gestione dei certificati SSL, che può essere costosa e complessa.

2. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL è il protocollo di sicurezza originale utilizzato per cifrare la comunicazione tra client e server. Oggi è stato sostituito dal più sicuro **TLS**, che fornisce un livello di protezione ancora maggiore.

• Cosa fa: TLS garantisce che le informazioni scambiate siano confidenziali (nessuno può leggere i

dati) e integre (i dati non possono essere modificati durante il trasferimento).
• Quando viene utilizzato: Viene utilizzato in HTTPS per proteggere la navigazione web, nei servizi di posta elettronica sicura, nelle comunicazioni VoIP e nelle VPN.

Pro: Fornisce una cifratura robusta, ed è utilizzato in molte applicazioni quotidiane. **Contro**: Le configurazioni TLS errate possono compromettere la sicurezza.

3. IPsec (Internet Protocol Security)

IPsec è un protocollo di sicurezza che opera a livello di rete, protetto da crittografia, ed è utilizzato per cifrare e autenticare i pacchetti IP durante il trasferimento.

• Cosa fa: Protegge i dati a livello di rete, assicurandosi che le comunicazioni tra dispositivi su una rete (sia privata che pubblica) siano sicure. IPsec può essere usato per implementare VPN sicure, che permettono di creare canali sicuri per il traffico dati.
• Quando viene utilizzato: È ampiamente usato nelle VPN (Virtual Private Networks) per garantire una connessione sicura su Internet.

Pro: Protegge a livello di rete, offrendo una sicurezza end-to-end. **Contro**: La configurazione di IPsec può essere complessa, soprattutto per i principianti.

4. SSH (Secure Shell)

Il **SSH** è un protocollo di rete che consente di accedere a un computer remoto in modo sicuro.

• Cosa fa: SSH cifra il traffico tra il client e il server, impedendo che i dati vengano intercettati o manipolati. È utilizzato principalmente per l'accesso remoto a server, la gestione delle risorse di rete e la configurazione sicura di dispositivi.
• Quando viene utilizzato: È comunemente utilizzato per l'amministrazione di server e dispositivi remoti, la gestione delle risorse in cloud e in ambienti di sviluppo.

Pro: Offre un modo sicuro per amministrare server remoti senza preoccuparsi che il traffico venga intercettato. **Contro**: Se non correttamente configurato, può essere vulnerabile agli attacchi di forza bruta.

5. WPA2 (Wi-Fi Protected Access II)

Il **WPA2** è un protocollo di sicurezza utilizzato per proteggere le reti wireless, ed è il più comune nelle reti Wi-Fi domestiche e aziendali.

• Cosa fa: WPA2 utilizza crittografia AES (Advanced Encryption Standard) per proteggere le informazioni che vengono trasmesse attraverso la rete Wi-Fi.
• Quando viene utilizzato: Viene utilizzato nelle reti Wi-Fi domestiche, aziendali e pubbliche per proteggere l'accesso alla rete e impedire che utenti non autorizzati possano intercettare il traffico.

Pro: Protegge le reti wireless in modo efficace con crittografia avanzata. **Contro**: Può essere vulnerabile ad attacchi come il cracking della password, se non vengono utilizzate password forti.

6. OAuth (Open Authorization)

OAuth è un protocollo di autorizzazione che consente a un'applicazione di ottenere l'accesso a risorse protette senza dover memorizzare le credenziali dell'utente.

• Cosa fa: Consente di delegare l'autorizzazione ad altre applicazioni, come quando si accede a un'app di terze parti utilizzando le credenziali di un account Google o Facebook.
• Quando viene utilizzato: È utilizzato per consentire l'accesso sicuro a API e servizi web senza

esporre le credenziali degli utenti.

Pro: Riduce il rischio di esposizione delle credenziali e semplifica l'accesso a servizi. **Contro**: Se non configurato correttamente, può esporre l'utente a rischi di sicurezza.
La sicurezza informatica è una delle principali preoccupazioni nel mondo digitale di oggi. Con l'aumento delle minacce online, proteggere i dati sensibili, le comunicazioni e i sistemi aziendali è diventato fondamentale. I **protocolli di sicurezza informatica** giocano un ruolo cruciale in questo processo, poiché definiscono le regole e le pratiche necessarie per garantire che le informazioni siano protette durante la trasmissione e l'archiviazione.

In questo articolo esploreremo i protocolli di sicurezza informatica più comuni e come contribuiscono a garantire la sicurezza nel cyberspazio. Tra questi, alcuni sono utilizzati per proteggere le comunicazioni, altri per gestire l'accesso a risorse sensibili, e altri ancora per difendere i sistemi contro attacchi esterni.

Cosa sono i protocolli di sicurezza informatica?

Un **protocollo di sicurezza informatica** è una serie di regole e linee guida che stabiliscono come proteggere i dati e le comunicazioni all'interno di una rete o tra dispositivi. Questi protocolli si occupano di gestire aspetti cruciali come la **confidenzialità**, **l'integrità** e la **disponibilità** delle informazioni, nonché la **autenticazione** e la **verifica dell'identità** degli utenti. Ogni protocollo ha uno scopo specifico e viene scelto in base al tipo di comunicazione o interazione che si vuole proteggere.

I protocolli di sicurezza più comuni

1. HTTPS (HyperText Transfer Protocol Secure)

Il **HTTPS** è il protocollo di sicurezza utilizzato per garantire la **sicurezza delle comunicazioni su Internet**. È una versione sicura dell'HTTP, che aggiunge uno strato di crittografia grazie all'uso del **SSL/TLS (Secure Sockets Layer/Transport Layer Security)**.

• Cosa fa: HTTPS cifra i dati scambiati tra il browser dell'utente e il server, impedendo che terze parti possano intercettare, leggere o manipolare le informazioni. Questo è particolarmente importante durante le transazioni bancarie online, l'inserimento di credenziali o l'acquisto di beni.
• Quando viene utilizzato: Ogni volta che si inseriscono informazioni sensibili su un sito web, come login, password o dati di pagamento.

Pro: Garantisce la protezione contro l'intercettazione delle comunicazioni. **Contro**: Richiede una gestione dei certificati SSL, che può essere costosa e complessa.

2. SSL/TLS (Secure Sockets Layer / Transport Layer Security)

SSL è il protocollo di sicurezza originale utilizzato per cifrare la comunicazione tra client e server. Oggi è stato sostituito dal più sicuro **TLS**, che fornisce un livello di protezione ancora maggiore.

• Cosa fa: TLS garantisce che le informazioni scambiate siano confidenziali (nessuno può leggere i dati) e integre (i dati non possono essere modificati durante il trasferimento).
• Quando viene utilizzato: Viene utilizzato in HTTPS per proteggere la navigazione web, nei servizi di posta elettronica sicura, nelle comunicazioni VoIP e nelle VPN.

Pro: Fornisce una cifratura robusta, ed è utilizzato in molte applicazioni quotidiane. **Contro**: Le configurazioni TLS errate possono compromettere la sicurezza.

3. IPsec (Internet Protocol Security)

IPsec è un protocollo di sicurezza che opera a livello di rete, protetto da crittografia, ed è utilizzato

per cifrare e autenticare i pacchetti IP durante il trasferimento.

• Cosa fa: Protegge i dati a livello di rete, assicurandosi che le comunicazioni tra dispositivi su una rete (sia privata che pubblica) siano sicure. IPsec può essere usato per implementare VPN sicure, che permettono di creare canali sicuri per il traffico dati.
• Quando viene utilizzato: È ampiamente usato nelle VPN (Virtual Private Networks) per garantire una connessione sicura su Internet.

Pro: Protegge a livello di rete, offrendo una sicurezza end-to-end. **Contro**: La configurazione di IPsec può essere complessa, soprattutto per i principianti.

4. SSH (Secure Shell)

Il **SSH** è un protocollo di rete che consente di accedere a un computer remoto in modo sicuro.

• Cosa fa: SSH cifra il traffico tra il client e il server, impedendo che i dati vengano intercettati o manipolati. È utilizzato principalmente per l'accesso remoto a server, la gestione delle risorse di rete e la configurazione sicura di dispositivi.
• Quando viene utilizzato: È comunemente utilizzato per l'amministrazione di server e dispositivi remoti, la gestione delle risorse in cloud e in ambienti di sviluppo.

Pro: Offre un modo sicuro per amministrare server remoti senza preoccuparsi che il traffico venga intercettato. **Contro**: Se non correttamente configurato, può essere vulnerabile agli attacchi di forza bruta.

5. WPA2 (Wi-Fi Protected Access II)

Il **WPA2** è un protocollo di sicurezza utilizzato per proteggere le reti wireless, ed è il più comune nelle reti Wi-Fi domestiche e aziendali.

• Cosa fa: WPA2 utilizza crittografia AES (Advanced Encryption Standard) per proteggere le informazioni che vengono trasmesse attraverso la rete Wi-Fi.
• Quando viene utilizzato: Viene utilizzato nelle reti Wi-Fi domestiche, aziendali e pubbliche per proteggere l'accesso alla rete e impedire che utenti non autorizzati possano intercettare il traffico.

Pro: Protegge le reti wireless in modo efficace con crittografia avanzata. **Contro**: Può essere vulnerabile ad attacchi come il cracking della password, se non vengono utilizzate password forti.

6. OAuth (Open Authorization)

OAuth è un protocollo di autorizzazione che consente a un'applicazione di ottenere l'accesso a risorse protette senza dover memorizzare le credenziali dell'utente.

• Cosa fa: Consente di delegare l'autorizzazione ad altre applicazioni, come quando si accede a un'app di terze parti utilizzando le credenziali di un account Google o Facebook.
• Quando viene utilizzato: È utilizzato per consentire l'accesso sicuro a API e servizi web senza esporre le credenziali degli utenti.

Pro: Riduce il rischio di esposizione delle credenziali e semplifica l'accesso a servizi. **Contro**: Se non configurato correttamente, può esporre l'utente a rischi di sicurezza.