HTTP

HTTP stands for Hypertext Transfer Protocol. This protocol can be used to transmit data across a network. The most important use of HTTP is the display of Internet pages. Without the protocol you wouldn't be able to access a website.

HTTP works according to the so-called client-server principle. The data is transferred between a web server and a web browser (also called a client). To access a website, the client (browser) sends a request (HTTP request) to the server. Using the URL (Uniform Resourse Locator), the client addresses a file on the server that the server should send to it. The request is then processed and answered with a response message. The simplest case of a response message is the display of the requested website.

HTTP vs HTTPS

Information transmitted via HTTP is unencrypted and appears in plain text. For more anonymity and secure data exchange on the Internet, there is an encrypted version of the protocol - HTTPS (Hypertext Transfer Protocol Secure). You can tell whether websites are being transmitted securely by looking at the URL. In this case, the beginning of the URL should be "https://" instead of "http://"

stand.

What is the difference between TLS and HTTPS?

HTTPS is an implementation of TLS encryption in addition to the HTTP protocol used by all websites as well as some other web services. Any website that uses HTTPS

therefore also uses TLS encryption.

What does Transport Layer Security (TLS) mean?

Transport Layer Security (TLS) is a widely used security protocol that facilitates privacy and data security for communications over the Internet. A primary use case of TLS is to encrypt communications between web applications and servers, e.g. E.g. web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging and Voice over IP (VOIP). In this article we will focus on the role of TLS in web application security.

TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organization. The first version of the protocol was published in 1999. The latest version is TLS

What is DNS?

The Domain Name System (DNS) is the phone book of the Internet. People access online information through domain names like nytimes.com or espn.com. Web browsers use Internet Protocol (IP) addresses to interact. DNS translates domain names into IP addresses so that browsers can load Internet resources.

How does DNS work?

For DNS resolution, a hostname (e.g. www.example.com) must be converted into an IP address that computers can understand (e.g. 192.168.1.1). Every device that connects to the Internet receives an IP address. This address is required to locate the device in question on the Internet - just as the postal address is used to locate a specific house. When a user wants to load a web page, what the user types into the web browser (example.com) must be translated into a machine-readable address so that the example.com web page can be found.

In order to understand the individual steps of DNS resolution, you need to know the various hardware components that a DNS query has to pass through. For the web browser, the DNS lookup happens in the background. No interaction is required from the user's computer other than the initial request.