Ποιες είναι οι διαφορές SSL/TLS vs STARTTLS;

Ioanna Anifanti - 2023-03-03 - Λοιπές

Πολλές φορές δημιουργείται σύγχυση μεταξύ των όρων SSL, TLS, και STARTTLS. Σε αυτό το άρθρο θα γίνει αναφορά στις διαφορές που υπάρχουν μεταξύ τους, ώστε να γίνουν ξεκάθαρες αυτές οι έννοιες.

Ποιες είναι οι διαφορές SSL/TLS vs STARTTLS;

SSL/TLS

Το **Secure Socket Layer (SSL)** και το **Transport Layer Security (TLS)** είναι και τα δύο **πρωτόκολλα ισχυρής κρυπτογράφησης** που παρέχουν ασφάλεια στην επικοινωνία σε ένα δίκτυο, όπως το Internet.

Τα συγκεκριμένα πρωτόκολλα χρησιμοποιούνται στην καθημερινότητά μας σε πλήθος εφαρμογών όπως στην περιήγηση μας στον παγκόσμιο ιστό, την υπηρεσία email, την μεταφορά αρχείων, την ανταλλαγή άμεσων μηνυμάτων, σε τηλεδιασκέψεις, VoIP κτλ. Το TLS είναι η συνέχεια του SSL πρωτοκόλλου.

Οι αριθμοί εκδόσεων SSL και TLS με σειρά από την παλαιότερη στη νεότερη είναι : SSL v2, SSL v3, TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3.

Όπως ήδη θα γνωρίζετε, οι εκδόσεις που υποστηρίζονται πλέον από την υποδομή μας είναι οι **TLS v1.2 & v1.3**. Οι υπόλοιπες εκδόσεις έχουν καταργηθεί λόγω γνωστών ευπαθειών.

Σε αυτό το άρθρο μπορείτε να δείτε με ποια έκδοση TLS είναι συμβατή η πλατφόρμα λογισμικού ή το λειτουργικό σύστημα που χρησιμοποιείτε.

STARTTLS

Το STARTTLS διαφέρει απο το SSL και το TLS καθώς δεν είναι πρωτόκολλο επικοινωνίας. Είναι μια **εντολή πρωτοκόλλου** που χρησιμοποιείται για να ενημερώσει τον email server ότι ο email client θέλει να αναβαθμίσει τη σύνδεση από μη ασφαλή σε ασφαλή σύνδεση, χρησιμοποιώντας SSL ή TLS πρωτόκολλο.

Πιο αναλυτικά, στο παρελθόν προτού εδραιωθεί η κρυπτογραφημένη μέθοδος επικοινωνίας με χρήση ασφαλών θυρών (πχ 587, 465, 995, 993), πολλές συνδέσεις μεταξύ ενός client και ενός server γινόταν με μη ασφαλή τρόπο, χρησιμοποιώντας τις default θύρες όπως η 25, 143 & 110. Αυτό έθετε σε κίνδυνο υποκλοπής και αλλοίωσης δεδομένων και σημαντικών πληροφοριών. Το STARTTLS ήρθε να βοηθήσει στη μείωση αυτού του κινδύνου, μετατρέποντας τη μη ασφαλή σύνδεση σε ασφαλή, με χρήση είτε SSL είτε TLS.

Με άλλα λόγια, το STARTTLS, χρησιμοποιεί τις θύρες 25, 143 & 110 αλλά με κρυπτογραφημένο τρόπο. Ο τρόπος που λειτουργεί είναι ο εξής: κατά την πρώτη επικοινωνία η σύνδεση πραγματοποιείται χωρίς κρυπτογράφηση και μετά ο client που στέλνει το email πρόκειται να ρωτήσει τον server εάν υποστηρίζει κάποια κρυπτογραφημένη μέθοδο. Εάν ο server υποστηρίζει κρυπτογραφημένη μέθοδο, τότε θα ξεκινήσει η επικοινωνία μεταξύ τους με κρυπτογράφηση. Αν ο server δεν υποστηρίζει κρυπτογραφημένη μέθοδο, τότε η σύνδεση δεν θα αναβαθμιστεί, και θα επιστρέψει στην αρχική επικοινωνία η οποία θα γίνει με μη ασφαλή τρόπο (κάτι το οποίο δεν συνίσταται για λόγους ασφαλείας και προστασίας προσωπικών δεδομένων). Αυτή η πρώτη επικοινωνία εμείς προτείνουμε να είναι πάντα secured γιατί στέλνονται πληροφορίες όπως username & password που δεν πρέπει να υποκλαπούν.

Ας αναφέρουμε ένα παράδειγμα. Κατά την SMTP επικοινωνία, αν η επικοινωνία γίνει στην θύρα 587 η σύνδεση είναι ασφαλής, το οποίο είναι και το ιδανικό. Εάν η σύνδεση γίνει στην θύρα 25, η σύνδεση είναι μη ασφαλής, όμως με χρήση STARTTLS, υπάρχει η δυνατότητα να σταλούν STARTTLS εντολές και να αναβαθμιστεί σε ασφαλή σύνδεση.