DIT172 | Project 3.1 | itp22104 | 7/12/2023

1. **Τι είναι Domain Validation (DV), Organization Validation (OV) και Validation (EV) certificates for authentication στο SSL/TLS;**

> - **DV** Επικυρώνει μόνο την ιδιοκτησία του domain.
> Η διαδικασία έγκρισης είναι αυτοματοποιημένη και αρκετά σύντομη, απαιτώντας από τον αγοραστή να επιδείξει μόνο τον έλεγχο του domain ή του URL. Αυτό γίνεται με το να στείλει ο CA ένα email στον ιδιοκτήτη του domain.
> - **OV** Επικυρώνει την ιδιοκτησία του domain και επίσης την ταυτότητα του οργανισμού ελέγχοντας το όνομα, τον τύπο, την κατάσταση και την φυσική διεύθυνσή του.
> - **EV** Είναι το πιο αυστηρό επίπεδο επικύρωσης. Επικυρώνει την ιδιοκτησία του domain και την ταυτότητα του οργανισμού, με επιπλέον αυστηρούς ελέγχους για στοιχεία όπως το δημόσιο τηλέφωνο της επιχείρησης, το χρόνο λειτουργίας της, τον αριθμό καταχώρησης και τη δικαιοδοσία. Πραγματοποιείται επίσης έλεγχος απάτης του domain, έλεγχος μαύρης λίστας επαφών και τηλεφωνική πιστοποίηση της εργασιακής θέσης του αιτούντος.
> Εμφανίζει το όνομα του οργανισμού στην μπάρα διεύθυνσης του προγράμματος περιήγησης.

---

2. **Τι είναι το Certificate Signing Request (CSR);**

> Είναι ένα από τα πρώτα βήματα προς την απόκτηση ενός πιστοποιητικού SSL/TLS. Το CSR περιλαμβάνει πληροφορίες (π.χ. κοινό όνομα, οργανισμός, χώρα) που ο CA θα χρησιμοποιήσει για τη δημιουργία του πιστοποιητικού. Περιλαμβάνει επίσης το δημόσιο κλειδί που θα ενσωματωθεί στο πιστοποιητικό και υπογράφεται με το αντίστοιχο ιδιωτικό κλειδί.

---

3. **Πως θα χειριζόσασταν το Heartbleed;**

> Θα άλλαζα όλα τα κλειδιά και τα πιστοποιητικά που μπορεί να έχουν διαρρεύσει λόγω του Heartbleed.
> Στη συνέχεια, θα ενημέρωνα τους χρήστες να αλλάξουν τους κωδικούς πρόσβασής τους και θα αναβάθμιζα σε έκδοση 1.0.1g ή μεταγενέστερη όπου θεωρούνται ασφαλείς από το πρόβλημα του Heartbleed.

---

4. **Τι είναι Perfect Forward Secrecy (PFS) στο πλαίσιο του SSL/TLS;**

> Είναι ένα είδος κρυπτογράφησης που επιτρέπει τις ανταλλαγές σύντομων, ιδιωτικών κλειδιών μεταξύ clients και servers. Αποτρέπει κακόβουλους χρήστες από το να αποκρυπτογραφήσουν δεδομένα από παρελθόντα ή μελλοντικά sessions, ακόμη και αν τα ιδιωτικά κλειδιά που χρησιμοποιούνται σε ένα συγκεκριμένο session κάποια στιγμή κλαπούν.

> Αυτό το πετυχαίνει χρησιμοποιώντας μοναδικά session keys, τα οποία δημιουργούνται αυτόματα κάθε φορά που γίνεται μια σύνδεση. Τα κλειδιά δεν χρησιμοποιούν προηγούμενες πληροφορίες κατά τη δημιουργία τους, εξαλείφοντας την ανάγκη για μακροπρόθεσμη αποθήκευση κλειδιών και αποτρέποντας την πρόσβαση σε ευαίσθητα δεδομένα με χρήση ήδη παραβιασμένων κλειδιών.

> Έτσι, οι κακόβουλοι χρήστες δεν μπορούν να αποκτήσουν το session key μέσω αποκρυπτογράφησης χωρίς εμπλοκή σε βασικό επίπεδο, με τον μηχανισμό συμφωνίας και ανταλλαγής κλειδιών, ο οποίος απαιτεί πολύ περισσότερη προσπάθεια από άλλες μεθόδους επίθεσης

---

5. **Πως λειτουργεί το HTTP Strict Transport Security (HSTS);**

> Είναι μια πολιτική ασφαλείας που επιβάλλει τη χρήση HTTPS αντί του ασφαλέστερου HTTP για την επικοινωνία με έναν διακομιστή. Αποτρέπει επιθέσεις όπως το man-in-the-middle και προστατεύει τους χρήστες από ασφαλέστερη σύνδεση.
> Όταν ένας χρήστης συνδέεται με έναν διακομιστή που υποστηρίζει το HSTS, ο διακομιστής επιστρέφει ένα header HSTS με την απόφαση του διακομιστή να απαιτεί τη χρήση HTTPS για τις μελλοντικές συνδέσεις. Αυτή η πληροφορία αποθηκεύεται στον browser του χρήστη.
> Από εκεί και πέρα, όταν ο ίδιος χρήστης προσπαθεί να συνδεθεί ξανά με τον ίδιο διακομιστή, ο browser αυτόματα χρησιμοποιεί το πρωτόκολλο HTTPS, αγνοώντας τυχόν προσπάθειες σύνδεσης μέσω του λιγότερο ασφαλούς HTTP.