SSL certifikáty

Ukončení podpory TLS 1.0 a TLS 1.1

V první polovině roku 2020 dojde k ukončení dvacet let starého protokolu TLS 1.0 a jeho osm let mladšího nástupce TLS 1.1. Tyto starší varianty jsou náchylné na různé druhy útoků, např. Poodle nebo Beast.

Za necelé 2 roky bude výchozí variantou v prohlížečích TLS 1.2, která vznikla před deseti lety, aby opravila chyby dvou předchozích návrhů. Změna se projeví u prohlížečů Chrome, Firefox, Edge a Safari.

Některé služby jako např. Gitlab oznámily, že podporu TLS 1.0 a 1.1 ukončí již koncem letošního roku.

Pro majitele/provozovatele serverů tato změna prakticky znamená, že nejpozději začátkem roku by jejich server měl mít podporu tohoto protokolu, jinak se klienti nebudou moci dostat k webům, které protokol TLS 1.2 nepodporují.

Pro uživatele by měl být dopad naprosto minimální - všechny aktuální verze browserů protokol podporují. Pokud používáte Internet Explorer ve verzi 10 nebo starší, Firefox 26 nebo starší případně Chrome 29 nebo starší, pak je nejvyšší čas zamyslet se nad upgradem. Některé webové služby Vám přestanou fungovat.

Další otázky a odpovědi:

Je nutné dekonfigurovat podporu TLS protokolů 1.0 a 1.1 na serveru ? V tuto chvíli to není nutné. Po odstranění podpory z browserů bychom tuto změni ale doporučili. Před konfigurační změnou si vždy ověřte, zda starší protokol nevyžaduje nějaký Vámi používaný software (například účetní systém importující data přes API apod)

Je třeba kontaktovat kvůli kontrole technickou podporu? Všechny managed servery bez podpory protokolu TLS 1.2 budeme v dostatečném předstihu sami kontaktovat. Pokud stávající operační systém umožní konfiguraci tohoto protokolu, bude třeba protokol pouze zapnout. U serverů s velmi starou softwarovou výbavou bude jediným řešení distribuční upgrade.

Musím to řešit, pokud nepoužívám na serverech https? Ne, webů bez zapnutého šifrování (https) se to nijak nedotkne. Ke zvážení je samozřejmě zda https na webech nezapnout.

Unikátní ID: #1103
Autor: Technicka podpora
Aktualizováno: 2018-11-12 13:54