maart 2023

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Transport Layer Security

Gebruikt uw organisatie de veiligste TLS-versie?

Wat is Transport Layer Security?

Transport Layer Security (TLS) is een protocol dat wordt gebruikt voor het opzetten van een beveiligde verbinding tussen twee computersystemen. TLS versleutelt de inhoud van onderlinge berichten en controleert de integriteit en authenticiteit van informatie. Het kent verschillende versies, waarvan alleen de nieuwste als veilig kan worden beschouwd. TLS is de opvolger van SSL (Secure Sockets Layer).

TLS wordt toegepast voor het beveiligen van vrijwel alle internetcommunicatie. Bijvoorbeeld bij het bezoek van een website, het gebruiken van een app op de telefoon, of bij het versturen van een e-mail. TLS wordt vaak gebruikt als een bouwsteen in de software: een stukje bekende, goed geteste code die voor softwareontwikkelaars beschikbaar is.

Waarom Transport Layer Security?

Als een verouderde versie van TLS wordt gebruikt is de kans groter dat kwaadwillenden, wanneer zij op het netwerk kunnen meekijken, de inhoud van informatie-uitwisseling kunnen inzien. Hierdoor kan gevoelige informatie (bijvoorbeeld persoonsgegevens, wachtwoorden of financiële gegevens) onbedoeld in verkeerde handen vallen.

Hoe weet u of uw organisatie actie moet ondernemen?

Gebruikt uw organisatie TLS-versie 1.1 of lager? Dan moet u direct ingrijpen!

- **Upgrade de software** of achterliggende libraries naar TLS 1.3 en configureer deze zodat oudere versies niet meer worden gebruikt.
- Voor software of libraries die vanuit legacy-overwegingen niet kunnen worden bijgewerkt: **implementeer een moderne proxyserver** die wel de juiste TLS versie en configuratie kan aanbieden. Deze kan daarna een 'onveilige' TLS connectie opzetten in het interne netwerk naar de applicatie. Behandel dit als een tijdelijke oplossing en maak alsnog afspraken met leveranciers voor een definitieve oplossing.
- **Quarantaine/isolatie.** Haal de applicatie van het internet af. Als de applicatie voor medewerkers beschikbaar moet blijven, dan kan deze beschikbaar worden gesteld via het interne netwerk. Denk hierbij aan zonering en afscherming. Behandel de applicatie als een beveiligingsrisico waarbij enkel strikt noodzakelijk in- en uitgaand verkeer wordt toegestaan vanaf specifieke netwerkadressen.

Gebruikt u TLS-versie 1.2?

Ook deze verouderde TLS-versie kan een risico vormen.

Is uw applicatie op internet aangesloten en beschikt over deze TLS-versie 1.2? Dit hoeft geen groot beveiligingsrisico op te leveren, mits de configuratie conform *best practices* is opgeleverd. Hierbij is het van grootte belang dat de juiste encryptie- en hashing algoritmen zijn ingesteld.

Gebruikt u TLS-versie 1.3?

Dan is uw applicatie voor nu veilig ingesteld.

Bepaal de TLS-versie van uw applicatie

Op dit moment zijn er zeven verschillende TLS-versies waarvan drie nog hun oude naam hebben, Secure Socket Layer (SSL). Deze versies kennen veilige en minder veilige instellingen. Vraag uw softwareleverancier om TLS 1.3 te ondersteunen als onderdeel van een toekomstvaste TLS-configuratie.

Versie	*Veiligheidsstatus*
TLS 1.3	Goed
TLS 1.2	Voldoende
TLS 1.1 TLS 1.0	Uit te faseren
SSL 3.0 SSL 2.0 SSL 1.0	Onvoldoende veilig

Check of uw organisatie de veiligste versie van TLS gebruikt.

Deze whitepaper *ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)* helpt uw organisatie te kiezen tussen alle mogelijke TLS-opties om zo te komen tot een veilige configuratie.

Whitepaper Richtlijnen TLS *(ncsc.nl)*