TRAFFIC LIGHT PROTOCOL (TLP)

Definice standardu FIRST a pokyny k použití

1. Úvod

a. Traffic Light Protocol (TLP) je protokol, který byl vytvořen s cílem usnadnit širší sdílení potenciálně citlivých informací a efektivnější spolupráci. Sdílení informací probíhá od *zdroje* informací směrem k jednomu nebo více *příjemcům*. TLP je sada čtyř štítků, které určují omezení sdílení, jež mají *příjemci* aplikovat. FIRST považuje za platné pouze štítky uvedené v tomto standardu.

b. Čtyři TLP štítky jsou: TLP:RED, TLP:AMBER, TLP:GREEN a TLP:CLEAR. V psané formě NESMÍ tyto štítky obsahovat mezery a MĚLY by být psány velkými písmeny. TLP štítky MUSÍ zůstat ve své původní podobě i když jsou použity v textu v jiných jazycích: obsah může být přeložený, avšak štítky být překládány nesmějí.

c. TLP poskytuje jednoduché a intuitivní schéma pro určení, s kým mohou být potenciálně citlivé informace sdíleny. TLP není formálním klasifikačním schématem. Protokol TLP nebyl vytvořen za účelem řešení licenčních podmínek, ani pravidel pro nakládání s informacemi nebo pro šifrování. TLP štítky a jejich definice nejsou určeny k ovlivňování svobodného přístupu k informacím nebo povinného zveřejňování informací v jakékoli jurisdikci.

d. TLP je optimalizován pro snadné osvojení, čitelnost pro člověka a sdílení informací mezi lidmi; může být rovněž použit v systémech automatizované výměny informací, jako je například MISP nebo IEP.

e. TLP je odlišný od Chatham House Rule[1], ale může být použit zároveň s ním, pokud je to vhodné. Zmíněné pravidlo stanoví, že při setkání, které se jím řídí, mohou jeho účastníci získané informace volně používat, ale nesmí vyzradit totožnost ani příslušnost řečníka (řečníků) ani jiného účastníka daného setkání.

f. Zdroj odpovídá za to, že příjemci informací označených TLP rozumí pokynům pro sdílení v TLP a mohou se jimi řídit.

g. Zdroj má možnost specifikovat další omezení sdílení. Příjemci je musí respektovat.

[1] https://www.chathamhouse.org/about-us/chatham-house-rule

h. Pokud příjemce potřebuje sdílet informace v širším rozsahu, než je určeno štítkem TLP, kterým byly označeny, musí získat výslovný souhlas od zdroje.

2. Použití

a. Jak používat TLP ve zprávách (jako je e-mail a chat)

Ve zprávách označovaných v souladu s TLP MUSÍ být TLP štítek, stejně jako jakákoli doplňující omezení, uveden přímo před samotnou informací. TLP štítek BY MĚL být uveden v předmětu e-mailu. V případě potřeby také nezapomeňte označit konec textu, k němuž se TLP štítek vztahuje.

b. Jak používat TLP v dokumentech

V dokumentech označovaných v souladu s TLP MUSÍ být TLP štítek, stejně jako jakákoliv doplňující omezení, uveden v záhlaví a zápatí každé stránky. Písmo použité na TLP štítek BY MĚLO být velikosti 12 b. nebo větší, aby bylo čitelné i pro uživatele se zhoršeným zrakem. TLP štítky je doporučeno zarovnávat vpravo.

c. Jak používat TLP při automatizované výměně informací

Použití TLP při automatizované výměně informací není definováno a je ponecháno na autorech systémů umožňujících takovou výměnu provádět. Použití však MUSÍ být v souladu s tímto standardem.

d. Kódy barev TLP v RGB, CMYK a Hex

	RGB: font			RGB: pozadí			CMYK: font				CMYK: pozadí				Hex: font	Hex: pozadí
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Poznámka ke kódům barev: pokud je mezi textem a pozadím příliš malý barevný kontrast, uživatelé se zhoršeným zrakem mají potíže se čtením textu nebo jej vůbec nevidí. TLP je navržen tak, aby vyhovoval i uživatelům se zhoršeným zrakem. Zdroje BY MĚLY dodržovat výše uvedené kódy barev, aby byl zajištěn dostatečný kontrast i pro tyto uživatele.

3. Definice pojmů v TLP

Komunita: Podle TLP je *komunita* skupina, která sdílí společné cíle, zkušenosti a v níž na neformální úrovni panuje vzájemná důvěra. Komunita může zahrnovat všechny odborníky na kybernetickou bezpečnost v určité zemi (nebo v sektoru či regionu).

Organizace: Podle TLP je *organizace* skupina, která sdílí společnou příslušnost na základě formálního členství a je vázána společnými zásadami stanovenými danou organizací. Organizace může zahrnovat i všechny členy organizace sdílející informace, ale jen zřídka je rozsáhlejší.

Klienti: Podle TLP jsou *klienti* osoby nebo subjekty, které využívají služby kybernetické bezpečnosti poskytované *organizací*. TLP:AMBER klienty standardně zahrnuje, takže příjemci takto označených informací je s nimi mohou dále sdílet, aby jim umožnili podniknout kroky k zajištění jejich ochrany. U týmů s celonárodní působností tato definice zahrnuje zúčastněné strany a cílové skupiny.[2]

a. TLP:RED = Pouze pro oči a uši *jednotlivých* příjemců – osob, bez možnosti dalšího sdílení. Zdroje mohou použít klasifikaci TLP:RED, pokud s informacemi nelze efektivně nakládat bez významného rizika pro soukromí, reputaci nebo činnost zúčastněných organizací. Příjemci proto nesmějí sdílet informace označené TLP:RED s nikým dalším. Například informace označené TLP:RED získané na konkrétní schůzce jsou určeny výhradně osobám, které se této schůzky samy účastnily.

b. TLP:AMBER = Možnost sdílení omezena, příjemci mohou takto označené informace šířit pouze na základě zásady "need-to-know"[3] v rámci své *organizace* a mezi její *klienty*. Povšimněte si, že TLP:AMBER+STRICT omezuje možnost sdílení pouze na *organizaci* samotnou. Zdroje mohou použít označení TLP:AMBER, pokud lze s informací efektivně nakládat pouze s další podporou, avšak případné sdílení informace mimo zúčastněné organizace s sebou nese riziko pro soukromí, reputaci nebo činnosti. Příjemci mohou sdílet informace označené TLP:AMBER se členy své vlastní organizace a jejími klienty, ale pouze na základě principu "need-to-know", aby zajistili ochranu své organizace, její klienty a zabránili případným dalším škodám. Poznámka: Pokud chce zdroj omezit sdílení **pouze** na samotnou organizaci, musí použít označení TLP:AMBER+STRICT.

c. TLP:GREEN = Možnost sdílení omezena, příjemci mohou takto označené informace šířit v rámci své komunity. Zdroje mohou používat označení TLP:GREEN, pokud je informace užitečná pro zvýšení povědomí v jejich širší komunitě. Příjemci mohou sdílet informace označené TLP:GREEN s kolegy a partnerskými organizacemi v rámci své komunity, avšak nesmí k tomu využívat veřejně přístupné kanály. Informace označené TLP:GREEN nesmějí být sdíleny mimo komunitu. Poznámka: Pokud „komunita" není definována, jedná se o odbornou komunitu v oblasti kybernetické bezpečnosti/obrany.

d. TLP:CLEAR = Příjemci mohou takto označené informace šířit po *světě*, sdílení není nijak omezeno. Zdroje mohou používat označení TLP:CLEAR pro informace, s nimiž je spojeno minimální nebo žádné předvídatelné riziko zneužití, v souladu s relevantními pravidly a postupy pro zveřejňování. S přihlédnutím k standardním autorským právům mohou být informace označené TLP:CLEAR sdíleny bez omezení.

---

[2] Termín cílové skupiny je zde použit ve zobecněném významu obdobně jako v dokumentu Popis Vládního CERT České republiky vytvořeného podle standardu RFC 2350.

[3] Zásada „need-to-know" požaduje, aby byl přístup k informacím omezen pouze na ty osoby, které z důvodu své pracovní náplně nebo povinností musí být s těmito informacemi obeznámeny nebo s nimi musí nakládat.

Poznámky:

1. Tento dokument používá termíny MUSÍ, MĚL a NESMÍ, jak jsou definovány v RFC-2119.
2. Připomínky nebo návrhy k tomuto dokumentu můžete zasílat na adresu tlp-sig@first.org.

Translation: Ondřej Nekovář, CSIRT-SPCSS/SPCSS s.p., CZ
Dana Třeštíková, CSIRT-SPCSS/SPCSS s.p., CZ
Marcel Danilov, CSIRT-SPCSS/SPCSS s.p., CZ
Review: Jan Pohl, CSIRT-SPCSS/SPCSS s.p., CZ
Věra Mikušová, CSIRT.CZ/CZ.nic z.s.p.o., CZ
Jan Kopřiva, FIRST liaison member, CZ