

NÚKIB



DOPORUČENÍ KE SDÍLENÍ INFORMACÍ

A PRÁCI S NIMI

Obsah

1 Úvod	3
2 Pravidla pro používání	4
2.1 Barevné provedení	4
2.2 Umístění	5
2.3 Písmo	5
3 Traffic Light Protocol (TLP)	6
3.1 Znění TLP protokolu v české verzi	6
3.2 TLP protokol v anglické verzi	7
4 Permissible Actions Protocol (PAP)	9
4.1 Znění PAP protokolu v české verzi.....	9
5 Příklady použití	10

1 Úvod

Toto doporučení určuje pravidla pro sdílení a práci s citlivými informacemi (dokumenty, indikátory kompromitace, zprávy). Doporučujeme tato pravidla značení používat pro chráněné, citlivé či jinak důvěrné informace, které je třeba kontrolovaně sdílet interně nebo s dalšími organizacemi.

Ke značení informací je vhodné využívat dvě kategorie značení, které mohou být užívány zvlášť i souběžně v rámci jedné informace:

- **Traffic Light Protocol (TLP)** určující pravidla pro sdílení informací.
- **Permissible Actions Protocol (PAP)** určující pravidla pro následné využití informací.

Práce s TLP a PAP je založena na dobrovolném respektování ze strany původců i adresátů informací za účelem zvýšení ochrany informací při jejich předávání a využití. **Před předáním informace označené dle tohoto doporučení je vždy nutné se ujistit, že je protistrana s aktuálními pravidly TLP nebo PAP seznámena a respektuje je.** V psaném textu se používají vizuální štítky, v mluveném projevu je vhodné říct „TLP“, resp. „PAP“ a poté danou úroveň.

Doporučení k používání protokolů TLP a PAP je přizpůsobeno potřebám Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Toto doporučení nenahrazuje náležitosti označování a nakládání s utajovanými informacemi ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, které je v případě utajovaných informací dle tohoto zákona nezbytné důsledně dodržovat.

2 Pravidla pro používání

Pro používání protokolů TLP a PAP platí stejná pravidla pro barevné provedení, umístění i písmo.

V psané formě nesmí tyto štítky obsahovat mezery a měly by být psány velkými písmeny. Pokud je to možné, měly by být štítky napsány barevně na černém pozadí (přesné barvy jsou uvedeny ve specifikaci od FIRST). Štítky musí zůstat ve své původní podobě, i když jsou použity v textu v jiných jazycích, tj. obsah může být přeložený, avšak štítky být překládány nesmějí.

Podrobná pravidla naleznete níže.

2.1 Barevné provedení

Výchozí barevné kódování jednotlivých příznaků a jejich pozadí v barevném prostoru HEX je následující:

Příznak	HEX	
	Text	Pozadí
TLP: RED PAP: RED	#FF2B2B	#000000
TLP: AMBER+STRICT	#FFC000	#000000
TLP: AMBER PAP: AMBER	#FFC000	#000000
TLP: GREEN PAP: GREEN	#33FF00	#000000
TLP: CLEAR PAP: CLEAR	#FFFFFF	#000000

Barevné kódování pro barevné prostory RGB a CMYK je dostupné na webu organizace FIRST.org.

Výchozí provedení příznaků je vždy na černém podkladu (tedy s černým zvýrazněním písma). Alternativně je možné uvést TLP příznaky bez černého zvýraznění.

Kromě příznaků TLP: CLEAR a PAP: CLEAR je možné pro ostatní příznaky použít alternativní barevné provedení, které se však může od výchozího barevného kódování lišit pouze sytostí a odstínem. Není tedy možné využít například modrou či fialovou barvu, průhlednost písma či jeho jiné stylizace atd. Například v případě TLP: GREEN se může jednat pouze o jiný odstín zelené barvy.

Vždy musí být dodržena barevná posloupnost v podobě tzv. „semaforu“ – viz výše.

Příznaky TLP: AMBER a TLP: AMBER+STRICT, resp. PAP: AMBER musí být vyhotoveny vždy ve vzájemně shodném barevném provedení.

Příznaky TLP: CLEAR a PAP: CLEAR je možné vyhotovit pouze v bílém či černém provedení (inverzním vůči zvýraznění písma či podkladu, na němž se nachází).

V případě definování alternativního barevného kódování jednotlivých příznaků a jejich případném (ne)zvýraznění musí být příznaky vždy jasně rozpoznatelné a čitelné.

Absence barevného provedení příznaků a zvolení jiných než níže uvedených variant písma (např. patkové) je možné pouze v ojedinělých případech a jen tehdy, kdy tyto parametry není možné v daném programovém prostředí zvolit.

2.2 Umístění

Příznak, TLP, PAP nebo oba současně, musí být v dokumentech, publikacích, analýzách a dalších obdobných materiálech umístěn v záhlaví a zápatí. V prezentacích je možné umístit příznak pouze do zápatí.

Není-li možné v odůvodnitelných případech umístit do dokumentu (např. smlouvy) popis jednotlivých příznaků, je nezbytné, aby s nimi byl příjemce informace seznámen jiným způsobem, např. alespoň odkázáním na příslušnou webovou stránku NÚKIB v doprovodném textu.

V e-mailové komunikaci musí být příznak umístěn na začátku a na konci těla e-mailové zprávy. Na konci těla e-mailové zprávy musí být příznak spojen s jeho krátkým popisem a odkazem na příslušnou webovou stránku NÚKIB.

2.3 Písmo

Jednotlivé znaky TLP, resp. PAP příznaků nesmí být prokládány mezerami. Za dvojtečkou v názvu příznaku by neměla být vložena mezera. Správný zápis vypadá takto: TLP:GREEN, nikoliv TLP: GREEN.

Font příznaků by měl být v bezpatkovém písmu bez jakéhokoliv dalšího formátování (kurzíva, přeškrtnutí, podtržení, atd.).

Příznaky musí být vždy uvedeny v kapitálkách.

Řez písma příznaků, stejně jako jeho font a varianta, by se měly vždy co nejvíce přibližovat výchozí podobě. Alternativní provedení musí vždy být jasně rozpoznatelné a čitelné.

Znění jednotlivých příznaků není možné překládat, vždy musí být v původním anglickém znění.

3 Traffic Light Protocol (TLP)

TLP slouží k určení míry důvěrnosti informací a možnosti jejich dalšího sdílení. Protokol vydává organizace FIRST.org, Inc, a aktuální verzi 2.0 v anglickém a českém jazyce naleznete zde: <https://www.first.org/tlp/>. Předchozí verze doporučujeme nevyužívat.

Za tímto účelem se informace označují jedním z pěti příznaků, které stanoví charakter informace a podmínky jejího použití. Doporučení k používání protokolu TLP vychází z aktuální verze TLP 2.0 a definice jednotlivých TLP příznaků jsou však **přizpůsobeny potřebám NÚKIB**. Požadavky organizace FIRST.org, mohou být v některých požadavcích na vizuální podobu TLP příznaků oproti tomuto doporučení otevřenější a benevolentnější. Určité upřesnění či zpřísnění jednotlivých požadavků má za cíl sjednocení využívání TLP v rámci NÚKIB.

Před zasláním informace označené dle protokolu TLP je vždy nutné se ujistit, že je protistrana s aktuálními pravidly TLP nebo PAP seznámena a respektuje je.

Je stanoveno následujících pět příznaků s uvedením charakteru informace a podmínkami jejich použití. V psaném textu se používají vizuální štítky, v mluveném projevu je vhodné říct „TLP“ a poté danou úroveň.

3.1 Znění TLP protokolu v české verzi

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol dostupnou na webových stránkách NÚKIB. Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Příznak	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují zásady need-to-know.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují zásady need-to-know.
TLP:GREEN	Informace může být sdílena v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

¹need-to-know — princip který tvrdí, že k informaci mají mít přístup pouze osoby, které danou informaci nutně potřebují ke svojí práci.

Zkrácené znění TLP protokolu pro e-mailovou komunikaci v české verzi

TLP:RED je určeno pouze pro osobu, která je příjemce informace a není možné ji šířit dál bez souhlasu původce. Více informací o TLP označení je k dispozici na webu NÚKIB.

TLP:AMBER+STRICT je určeno pouze pro organizaci příjemce informace, a to pouze pro osoby s need-to-know. Více informací o TLP označení je k dispozici na webu NÚKIB.

TLP:AMBER je určeno pro organizaci příjemce informace a její partnery, a to pouze pro osoby s need-to-know. Více informací o TLP označení je k dispozici na webu NÚKIB.

TLP:GREEN je určeno pro organizaci příjemce informace a její partnery, přičemž není možné ji sdílet skrze veřejně dostupné kanály. Více informací o TLP označení je k dispozici na webu NÚKIB.

TLP:CLEAR je možné poskytovat a šířit bez omezení. Více informací o TLP označení je k dispozici na webu NÚKIB.

3.2 TLP protokol v anglické verzi**TERMS OF USE**

The information provided shall be used in accordance with the Traffic Light Protocol methodology available at the NÚKIB website. The information is marked with a TLP label, which sets out terms and conditions for the use of the information. The individual TLP labels are specified below and indicate the nature of the information and the terms and conditions for their use:

Label	Terms of use
TLP:RED	The information is for the eyes and ears of individual recipients only. It cannot not be provided to any person other than the person to whom the information was addressed unless the other persons are explicitly identified. If the recipient finds important to disclose the information to other bodies, this have to be done only with the consent of the originator of the information.
TLP:AMBER+STRICT	The information can only be shared and spread within the organization of the recipient and only to those individuals who meet need-to-know ¹ principle.
TLP:AMBER	The information can only be shared and spread within the organization of the recipient and its partners and only to those individuals who meet need-to-know principle.
TLP:GREEN	The information can be shared and spread within the organization of the recipient and, where appropriate, with partners of the recipient. However, not via publicly available channels; the recipient must ensure the confidentiality of the communication when passing the information.
TLP:CLEAR	The information can be disclosed without any restriction. Restrictions based on the intellectual property rights of the originator and/or recipient, or third parties are not affected by this provision.

¹Need-to-know - a principle that states that only individuals who absolutely need the information for their work should have access to it.

Zkrácené znění TLP protokolu pro e-mailovou komunikaci v anglické verzi

TLP:RED is for the eyes and ears of individual recipients only. It cannot not be provided to any person other than the person to whom the information was addressed without the consent of the originator of the information. More information about TLP labels is available at the NÚKIB website.

TLP:AMBER+STRICT can only be shared and spread within the organization of the recipient and only to those individuals who meet need-to-know principle. More information about TLP labels is available at the NÚKIB website.

TLP:AMBER can only be shared and spread within the organization of the recipient and its partners and only to those individuals who meet need-to-know principle. More information about TLP labels is available at the NÚKIB website.

TLP:GREEN can be shared within the organization of the recipient and its partners, however not via publicly available channels. More information about TLP labels is available at the NÚKIB website.

TLP:CLEAR can be disclosed without any restriction. More information about TLP labels is available at the NÚKIB website.

4 Permissible Actions Protocol (PAP)

PAP slouží k určení možností práce s informacemi jako např. jejich využití pro monitoring či blokování. Původní specifikace tohoto značení je dostupná na https://www.misp-project.org/taxonomies.html#_pap.

PAP je vhodné využít zejména v případech, ve kterých jsou sdíleny indikátory kompromitace (IP adresy, domény, hashe), případně informace, které mohou být použity k detekci nebo blokování útočníka.

Jsou stanoveny následující čtyři příznaky s uvedením charakteru informace a podmínkami jejich použití. V psaném textu se používají vizuální štítky, v mluveném projevu je vhodné říct „PAP“ a poté danou úroveň.

4.1 Znění PAP protokolu v české verzi

PODMÍNKY VYUŽITÍ INFORMACÍ

Využití poskytnutých informací probíhá v souladu s metodikou Permissible Actions Protocol dostupnou na webových stránkách NÚKIB. Informace je označena příznakem, který stanoví podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Příznak	Podmínky použití
PAP:RED	Při nakládání s informací lze provádět pouze akce, které nejsou zjistitelné. Příjemci nesmí informaci aktivně využívat v sítích připojených k internetu, ale pouze pasivně v kontrolované infrastruktuře určené pro investigace. ¹
PAP:AMBER	Při nakládání s informací lze provádět pouze pasivní akce. Příjemci mohou např. vyhledávat informaci prostřednictvím třetích stran (např. WHOIS nebo CESNET NERD), mohou vyhledávat informaci v napadené síti nebo mohou využít honeypot pro monitoring.
PAP:GREEN	Při nakládání s informací lze mimo svou infrastrukturu provádět pouze neinvazivní akce, ve své infrastruktuře lze provádět libovolné akce. Příjemci mohou informaci použít např. pro ping na cíl, blokaci příchozí/odchozí komunikace z/na cíl či specificky nakonfigurovat honeypot pro interakci s cílem.
PAP:CLEAR	Žádné omezení pro nakládání s informací. Tím nejsou dotčeny případné povinnosti vyplývající z právních předpisů.

¹Je důležité dávat pozor, aby používané nástroje neodesílaly data do internetu skrytě (např. dotazování WHOIS databáze). Cloudové služby je možné používat pouze v případě, pokud je smluvně ošetřena důvěrnost zpracovaných informací.

5 Příklady použití

Příznaky	Možný scénář
TLP:RED + PAP:RED	Od partnerů jsme získali informaci, že APT skupina má přístup do vaší sítě. Prozatím se nepokoušejte útočnicka ve vaší síti vyhledávat, můžete však některou z napadených stanic forenzně analyzovat.
TLP:AMBER+STRIC T + PAP:GREEN	Z našich zjištění vyplývá, že je ve vaší síti používána zranitelná verze firewallu. Doporučujeme co nejdříve provést jeho aktualizaci. Tuto informaci je možné předat pouze v rozsahu vaší organizace, a to pouze osobám, které splňují need-to-know.
TLP:AMBER + PAP:AMBER	Od partnerů jsme získali informaci, že APT skupina má přístup do vaší sítě. Prozatím proveďte prověření vaší sítě a zjistěte rozsah napadení, útočnicka nijak neblokuje ani s ním nijak neinteragujte. Tuto informaci můžete předat osobám, které splňují need-to-know, ať v rámci vaší organizace, nebo také správci či dodavateli IT, kteří tuto informaci potřebují pro výkon své práce.
TLP:GREEN + PAP:AMBER	Z našich zjištění vyplývá, že se APT skupina pokouší útočit na zdravotnická zařízení, v příloze naleznete způsob, jak útočnicka detekovat. V případě detekce útočnicka neblokuje, ale kontaktujte nás.
TLP:GREEN + PAP:CLEAR	V České republice nyní probíhá phishingová kampaň zaměřující se na zdravotnická zařízení, poučte své uživatele o možných rizicích.
TLP:CLEAR + PAP:CLEAR	GovCERT.CZ za poslední rok řešil 126 incidentů, z toho 26 závažných.

Datum	Verze	Změněno (jméno)	Změna
2.6.2025	1.0	NÚKIB	Vytvoření dokumentu