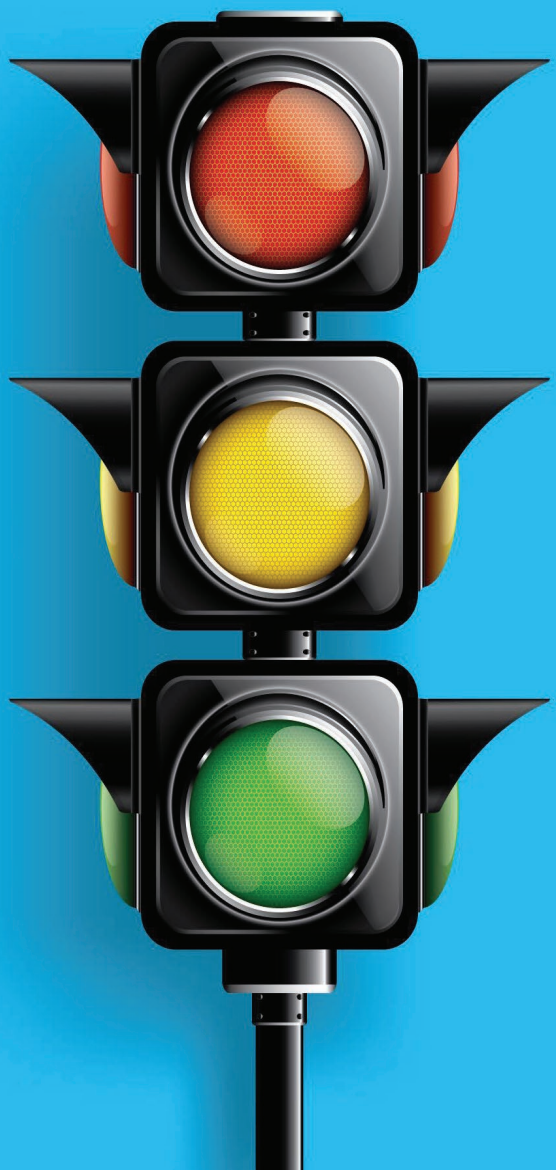


SEMAFOROVÝ PROTOKOL

Semaforový protokol (The Traffic Light Protocol - TLP) je mechanizmus na označenie povolenej distribúcie informácií. Používa sa v komunitách pri zdieľaní informácií.

Pôvodca informácií má povinnosť „signalizovať", do akej miery chce, aby sa tieto informácie šírili mimo komunity.
Cieľom iniciatív spojených so semaforovým protokolom je podporiť výmenu a disribúciu citlivých informácií medzi organizáciami.

Citlivé informácie potrebujú citlivú manipuláciu

Ak publikujete, zdieľate, komunikujete alebo len preposielate informácie, ktoré môžu byť potenciálne citlivej povahy, určite ste už stáli pred otázkou ako ľahko a stručne vyjadriť

- citlivosť zdieľaných informácií
- ako môže prijímateľ využiť či šíriť zdieľané informácie.

A práve na to slúži semaforový protokol.

Protokol je založený na označení informácie jednou zo štyroch farieb. Cieľom je vyjadriť, ako môže príjemca ďalej šíriť informáciu, a či to vôbec môže vykonať. Ak príjemca, či príjemcovia vyžadujú rozsiahlejšie šírenie, musia konzultovať s pôvodcom informácie.

Použite štítok!

Informáciu, ktorú zdieľate, jednoducho označíte podľa protokolu. Priložíte príslušný farebný štítok a ten indikuje limity, ktoré musí prijímateľ dodržať v ďalšom šírení informácie.

TLP:RED, **TLP:AMBER**, **TLP:AMBER+STRICT**, **TLP:GREEN** a **TLP:CLEAR**.

Znenie štítku v písomnej forme nemusí obsahovať medzery v označení. Zároveň označenia podľa semaforového protokolu musia zostať v pôvodnej podobe vo všetkých jazykoch, kde sa používajú.

Význam štítkov je intuitívne zrejmý aj laikovi a jednotné používanie zjednodušuje prijímateľovi prácu s prijatými informáciami.

Distribúcia informácii podľa farieb štítkov

RED (ČERVENÁ)

Informácia určená iba pre vymenovaných príjemcov.

Napríklad pri prezenčnom alebo online stretnutí sú takto označené informácie vymedzené na prítomné respektíve pozvané osoby. Vo väčšine prípadov sú RED informácie odovzdané ústne, najlepšie osobne.

AMBER (JANTÁROVÁ)

Limitovaná distribúcia informácie.

Príjemca môže zdieľať informácie s osobami v rámci svojej organizácie vrátane klientov vždy na základe princípu *need-to-know.*

AMBER+STRICT

V tejto podkategórii je distribúcia informácie limitovaná.

Príjemca môže zdieľať informácie s osobami výhradne v rámci organizácie. Pôvodca by mal určiť obmedzenia zdieľania.

GREEN (ZELENÁ)

Informácia distribuovaná v komunite.

Informácie v kategórii GREEN sa môžu šíriť v konkrétnej skupine osôb, nesmú sa však publikovať na internete, ani akokoľvek zverejňovať mimo komunity.

CLEAR (respektíve BIELA)

Informácia distribuovaná neobmedzene.

V súlade so štandardnými pravidlami o autorských právach môžu byť CLEAR informácie šírené voľne bez obmedzenia.

Skupiny prijímateľov

V semaforovom protokole v súvislosti s označením AMBER a GREEN sú skupiny prijímateľov definované nasledovne:

- Komunita (community)

  Skupina, ktorá zdieľa spoločné ciele, postupy a neformálne vzťahy založené na dôvere. Komunita môže byť až taká široká, že zahŕňa napríklad všetkých odborníkov v oblasti kybernetickej bezpečnosti v krajine, v sektore či regióne.

- Organizácia (organization)

  Skupina, definovaná spoločnou príslušnosťou cez formálne členstvo alebo pracovnú zmluvu, viazaná spoločnými zásadami či pravidlami stanovenými touto organizáciou. Organizácia môže byť taká rozsiahla, že zahŕňa všetkých jej členov, respektíve zamestnancov. Typicky sa však informácie zdieľajú len v časti organizácie.

- Klienti (clients)

  Ľudia alebo subjekty, ktorým organizácia poskytuje služby. Pre tímy s národnou zodpovednosťou zahŕňa táto definícia všetky zainteresované strany.

Citlivé informácie by mali byť v čase zverejnenia označené v súlade so semaforovým protokolom.

Všetky citlivé informácie sú považované za AMBER, pokiaľ nie je uvedené inak. Štandardne a pokiaľ nie je v čase zverejnenia uvedené inak, totožnosť zdroja citlivých informácií bude vždy označená ako RED.

Semaforový protokol môže byť prispôsobený na použitie v rámci organizácie. Napríklad tam, kde je povolený úplný prístup k všetkým zdieľaným informáciám len niektorým konkrétnym osobám.

RGB hodnoty TLP farieb

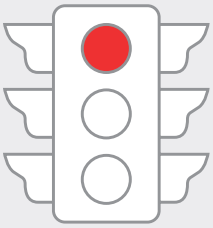
- **Správa elektronickej pošty** označená podľa semaforového protokolu by mala uvádzať TLP farbu informácie v predmete správy a aj pred samotnou informáciou v tele e-mailu. Farba musí byť uvedená veľkými písmenami: TLP:RED, TLP:AMBER, TLP:GREEN alebo TLP:WHITE.
- **Dokumenty** označené podľa protokolu by mali uvádzať TLP farbu v hlavičke a v päte každej strany. Aby sa predišlo zámene s existujúcimi klasifikačnými schémami, odporúča sa správne toto označenie odôvodniť. TPL farba by sa mala zobrazovať veľkými písmenami a veľkosťou 12 bodov alebo viac.
- **Pri automatizovaných výmenách informácií** nie je používanie protokolu definované, je to ponechané na tvorcoch systémov, ale musí byť v súlade s touto normou.

TLP: RED:	TLP:RED: R=255, G=43, B=43, pozadie: R=0, G=0, B=0
TLP: AMBER	TLP:AMBER: R=255, G=192, B=0, pozadie: R=0, G=0, B=0
TLP: GREEN	TLP:GREEN: R=51, G=255, B=0, pozadie: R=0, G=0, B=0
TLP: CLEAR	TLP:WHITE: R=255, G=255, B=255, pozadie: R=0, G=0, B=0

Spôsob označovania informácií pri ich výmene informácií organizáciami rieši technická norma ISO/IEC 27010:2015 *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications.*

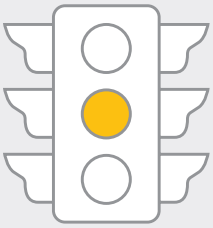
Podrobnosti použitia použitia TLP protokolu sú dostupné na: https://www.first.org/tlp/

Existuje niekoľko mierne odlišných spôsobov použitia semaforového protokolu. Tento opis je prevzatý z Príručky najlepšej praxe výmeny informácií o bezpečnosti sietí, ktorú vydala Európska agentúra pre kybernetickú bezpečnosť ENISA. Koncept bol pôvodne vyvinutý britským Centrom pre ochranu národnej infraštruktúry (CPNI).



TLP:RED

Distribúcia iba medzi dvoma subjektami bez možnosti ďalšieho šírenia. Príjemca nemože šíriť informácie mimo stretnutia alebo skupiny, v ktorej sa o informácii dozvedel.



TLP:AMBER

TLP:AMBER +STRICT

Distribúcia v určitej uzavretej skupine alebo zákazníkom, pre ktorých je informácia určená. Príjemca môže šíriť informácie s týmto označením vo svojej organizačnej alebo zákazníckej štruktúre.

TLP:AMBER+STRICT sa používa pri distribúcii len v rámci organizácie.

TLP:GREEN

Distribúcia v rámci sektora alebo určitej komunity, ide o neverejné informácie.

TLP:CLEAR

Distribúcia bez obmedzení, čiže informácie sú klasifikované ako verejné.

Spolufinancovaný Európskou úniou

Financované Európskou úniou. Vyjadrené názory a postoje sú názormi a vyhláseniami autora(-ov) a nemusia nevyhnutne odrážať názory a stanoviská Európskej únie. Európska únia za ne nepreberajú žiadnu zodpovednosť.

NCC-SK SLOVAKIA CYBERSECURITY COORDINATION CENTRE

Kompetenčné a certifikačné centrum kybernetickej bezpečnosti

ISBN 978-80-69011-04-5

Verzia V.1

www.cybercompetence.sk