Kraj Vysočina
KRAJSKÝ ÚŘAD KRAJE VYSOČINA
Odbor informatiky
Žižkova 57, 587 33 Jihlava, Česká republika

Zásady pro udělování a užívání značky „Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET“

verze leden 2015

1. Cíl značky

Značka „Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET“ byla vytvořena v souvislosti s činností odboru informatiky Krajského úřadu Kraje Vysočina v oblasti elektronické bezpečnosti. Na semináři k problematice elektronické bezpečnosti, který se konal v dubnu 2011 a v únoru 2012, byla vyjádřena podpora myšlence vytvoření značky elektronické bezpečnosti. V roce 2014 se rozhodla pracovní skupina zásady aktualizovat.

Spolupráce s poskytovateli internetového připojení a dalšími subjekty působícími v oblasti ICT (prodejci hardwaru, softwaru, tvůrci softwaru nebo webových stránek) je z pohledu uživatelů resp. zákazníků velmi důležitá, jelikož oni jsou velmi často prvními, s kým se uživatel při pořizování internetového připojení, technického vybavení a software setkává. A tedy je nutné, aby se právě od nich dozvěděl o nástrahách a problémech, které mohou při nedostatečném zabezpečení a neuváženém používání nastat.

Cílem značky je tedy přispět k zajištění elektronické bezpečnosti uživatelů elektronických služeb a propagace této problematiky mezi uživateli především na území Kraje Vysočina.

2. Pracovní skupina pro elektronickou bezpečnost

O udělení práv k užívání značky rozhoduje Pracovní skupina pro elektronickou bezpečnost Kraje Vysočina (dále jen pracovní skupina). Jejími členy jsou vedle pracovníků krajského úřadu z odboru informatiky, školství a sociálních věcí, také odborní pracovníci z řad Policie ČR, Vyšší policejní školy MV v Praze, Krajské hospodářské komory Kraje Vysočina, Okresního státního zastupitelství v Jihlavě, příspěvkové organizace Vysočina Education, dále pak odborníci z Národního centra bezpečnějšího internetu, sdružení NIC.CZ, sdružení CESNET, Národního bezpečnostního úřadu a společnosti AutoCont Jihlava.

Pracovní skupina zasedá zhruba každé 2 měsíce. Informace o práci skupiny jsou k dispozici na stránkách www.kr-vysocina.cz/ebezpecnost.

3. Postup při udílení značky

Držitelem značky může být právnická i fyzická osoba. Značka bude přidělena, jestliže, subjekt působící v oblasti ICT, resp. poskytovatel internetového připojení splní níže zmíněná kritéria. Pracovní skupina může zamítnout udělení značky žadateli nebo značku dodatečně odejmout, jestliže je jeho vystupování v rozporu se

zásadami a cílem značky, odporuje morálním a etickým zásadám, obecnému estetickému cítění nebo by mohl jinak poškodit dobré jméno značky nebo Kraje Vysočina.

Žadatel (poskytovatel internetového připojení, resp. další subjekt působící v oblasti ICT) obdrží od Krajského úřadu Kraje Vysočina (dále jen koordinátor) formulář žádosti o značku (viz příloha č. 1), který vyplní a odevzdá na podatelnu Krajského úřadu Kraje Vysočina, Žižkova 57, Jihlava popř. elektronicky na adresu bezpecny-internet@kr-vysocina.cz.

Koordinátor zkontroluje formální správnost a úplnost vyplněné žádosti a případně požádá žadatele o její doplnění nejpozději do 15-ti dnů po jejím obdržení.

Koordinátor předá všechny žádosti pracovní skupině alespoň 7 dní před jejím zasedáním. Pracovní skupina posoudí, jestli žadatel splnil daná kritéria a rozhodne o přidělení nebo nepřidělení značky.

V případě kladného rozhodnutí bude žadatel informován dopisem hejtmana Kraje Vysočina do 1 měsíce od schválení přidělení značky.

V případě záporného rozhodnutí uvědomí koordinátor žadatele a sdělí mu důvody zamítnutí žádosti.

Na udělení značky není právní nárok.

Koordinátor i pracovní skupina budou postupovat v souladu se zákonem č. 101/2000 Sb., o ochraně osobních údajů. Koordinátor si vyhrazuje právo zveřejnit informace poskytnuté žadatelem v souvislosti s žádostí o udělení značky.

4. Kritéria pro žadatele

Žadatelé, kteří chtějí užívat značku „Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET“ musí splnit následující kritéria:

1. Živnostník, firma, organizace mající kvalifikaci pro poskytování služeb v oblasti ICT

   Způsob doložení: předložení kopie živnostenského listu, výpisu z rejstříku firem, apod. (nemusí být úředně ověřeno ani v originálu)

2. Poskytování služeb na území Kraje Vysočina

   Způsob ověření: čestné prohlášení žadatele s informací o územní působnosti

3. Popis produktu(ů) a služeb naplňujících myšlenku elektronické bezpečnosti s následujícími podmínkami a parametry (alespoň jedna podmínka)

   a. Pro poskytovatele internetového připojení

- zabezpečené rozhraní k veřejné síti (centrální firewall, NAT, IDS, IPS)
- monitoring a sběr provozních dat (Netflow s možností volby ze strany zákazníka)
- aktivní upozorňování na nestandardní síťový provoz ze strany klienta nebo vůči klientovi
- zabezpečený internet pro děti (filtrace, blacklisty, předkofigurovaný router/firewall)
- aktivní spolupráce s CSIRT.CZ (hlášení bezpečnostních incidentů)
- zapojení v projektu FENIX (NIX.CZ)
- poskytování připojení přes IPv6
- vedení DNS záznamů v DNSSEC
- školení klientů v oblasti el. bezpečnosti

b. Pro prodejce hardwaru

- školení klientů v oblasti el. bezpečnosti
- poskytování služeb v oblasti bezpečného nasazení zakoupeného HW
- změny defaultních nastavení zařízení a systémů
- podněcování interakce a zpětné vazby v komunitě uživatelů/zákazníků
- prodej HW zařízení s bezpečnostní certifikací
- nabídka komplexních řešení elektronické bezpečnosti pro firmy/domácnosti
- předinstalace bezpečnostních SW (anti-x, firewall, …) na HW
- doporučení ohledně základního bezpečnostního nastavení (změna default parametrů - heslo ...)
- update firmware v zařízení na verzi z pohledu výrobce bez zranitelností
- předávání informací ohledně možných rizik v souvislosti s provozem zařízení (odhalené bezpečnostní hrozby)

c. Pro prodejce a tvůrce softwaru

- školení klientů v oblasti el. bezpečnosti
- nabídka služeb bezpečného nasazení dodávaného SW
- penetrační a zátěžové testy SW řešení v prostředí zákazníka
- nabídka pravidelné profilaxe nasazeného SW

- bezpečnostní certifikace dodávaného SW
- podněcování interakce a zpětné vazby v komunitě uživatelů/zákazníků
- doporučení ohledně základního bezpečnostního nastavení (změna default parametrů - heslo ...)
- informace ohledně „dobré praxe“ tzn. popis reálných nasazení daného softwaru u různých zákazníků (možnost referencí)
- informace o klíčových aktualizacích, o nových verzích a novinkách v nich, včetně informací o připravovaných funkcionalitách (prostředník mezi dodavatel a zákazníkem)
- informace o reálných případech (ideálně) v ČR, kde došlo k případným průnikům, ztrátám dat, ohrožení bezpečnosti z důvodu např. neaplikování bezpečnostních zásad (hesla, updaty, nové verze software, vysoká oprávnění uživatelů, sociální útoky atd.)

d. Pro tvůrce webových stránek, poskytovatele webového obsahu a poskytovatele webhostingu

- penetrační a zátěžové testy webové aplikace
- testy na obecně známé zranitelnosti (např. testy xss, sql injection, rfi, lfi, code upload nebo OWASP top 10).
- dostupnost popř. zasílání systémových a bezpečnostních logů
- pravidelná profylaktická kontrola webové aplikace
- filtrace provozu pomocí pokročilých technik (IPS, webový aplikační firewall)
- dostupnost zálohované konektivity (PI IP adresy, autonomní systém)
- pravidelná kontrola platnosti a korektnosti šifrovacích certikátů
- dostupnost bezpečných platebních mechanismů
- podpora provozu služeb na IPv6 a DNSSEC

Způsob ověření: předložení dokumentů prokazujících splnění těchto požadavků, detailní popis produktu nebo služby – posouzení jejích splnění Pracovní skupinou eBezpečnosti.

5. Užívání značky

Právo na užívání značky je nepřenosné a neprodejné. Značka je přidělena na 2 roky od data vystavení. Nejpozději 1 měsíc před uplynutím této lhůty je nutné podat žádost o udělení značky znovu. Žádost o opětovné udělení značky musí obsahovat i zprávu o aktivitách žadatele v oblasti el. bezpečnosti za období užívání značky.

Po dobu platnosti udělení značky garantuje uživatel značky nepřetržité plnění kritérií, která uvedl v žádosti, a je povinen hlásit koordinátorovi jakékoliv změny skutečností uvedených v žádosti, a to písemně (případně e-mailem) nejpozději do 3 týdnů od vzniku změny. V případě závažné změny koordinátor postoupí informaci pracovní skupině, která rozhodne o nutnosti znovu projednat platnost přidělení značky.

6. Úspěšný žadatel se zavazuje k následujícím aktivitám:

1. Propagace značky na svých webových stránkách, předávání materiálů o elektronické bezpečnosti zákazníkům, propagace bezpečnostních standardů u jednotlivých zákazníků

   Způsob ověření: čestné prohlášení žadatele, zpětná vazba zákazníků

2. Hlášení bezpečnostních incidentů z oblasti elektronické bezpečnosti koordinátorovi nebo CSIRT.CZ

   Způsob ověření: čestné prohlášení žadatele

3. Zajistit pravidelné vzdělávání pracovníků žadatele v oblasti el. bezpečnosti. Nejméně jedenkrát během dvou let se žadatel nebo jeho pracovníci zúčastní semináře k problematice el. bezpečnosti, který pořádá Kraj Vysočina nebo odborného semináře, který pořádá CSIRT.CZ popř. NIC.CZ

   Způsob ověření: čestné prohlášení žadatele poté, co se žadatel nebo jeho pracovníci zúčastní semináře.

4. Zveřejnit na svých internetových stránkách informace o produktu, který naplňuje myšlenku elektronické bezpečnosti a informace o tom, co sám žadatel dělá v oblasti elektronické bezpečnosti

   Způsob ověření: čestné prohlášení žadatele

5. V rámci vlastních aktivit informovat o projektu eBezpečnosti Kraje Vysočina

   Způsob ověření: čestné prohlášení žadatele

7. Kraj Vysočina úspěšným žadatelům poskytne:

1. Materiály o elektronické bezpečnosti pro zákazníky, minimální bezpečnostní standardy
2. Banner, samolepky - značky „Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET“
3. Zajištění vzdělávání pro zaměstnance úspěšného žadatele – organizace seminářů
4. Aktualizace minimálních bezpečnostních standardů
5. Propagace firmy na internetových stránkách Kraje Vysočina www.kr-vysocina.cz/ebezpecnost (konkrétně ve složce „Bezpečný internet“ a také na portálu www.kr-vysocina.cz/kamseobratitsproblemy)

Koordinátor může žadatelem dojednat individuálně zvláštní podmínky. Držitel značky může používat značku také dalšími způsoby, např. na hlavičkovém papíře, reklamních materiálech, vizitkách, webových stránkách, apod.

8. Kontrola

Kontrolu plnění daných kritérií budou vykonávat sami zákazníci, kteří budou mít možnost nahlásit případné nedostatky na krajský úřad (písemně nebo elektronicky na adresu bezpecny-internet@kr-vysocina.cz), a pracovní skupina se bude tímto oznámením zabývat a případně koordinátor provede sám kontrolu.

9. Užívání značky dalšími subjekty

Značku mohou používat na základě čestného prohlášení. S krajským úřadem i další subjekty (instituce státní správy, samosprávy, nevládní organizace, apod.) sídlící v regionu, které tak mohou podpořit propagaci nebo dobré jméno značky.

O možnostech a podmínkách užívání značky bude jednat koordinátor s každým subjektem individuálně.

10. Postup při porušení zásad

Při zjištění porušení zásad nebo kritérií vyzve koordinátor uživatele značky k nápravě v přiměřené lhůtě nebo rozhodne o odebrání značky. Rozhodnutí o odebrání značky potvrdí pracovní skupina při nejbližším zasedání.

Při neoprávněném užití značky bude postupováno soudní cestou.

11. Závěrečná ustanovení

Tyto zásady vstupují v platnost dne 12. ledna 2015.

Případné změny zásad a kritérií mohou být provedeny po dohodě koordinátora s pracovní skupinou.