Doporučení k využívání doménových certifikátů pro webové aplikace přístupné veřejnosti

portal.neweb.govcert.cz/informacni-servis/aktuality/doporuceni-k-vyuzivani-domenovych-certifikatu-pro-webove-aplikace-pristupne-verejnosti

TLP:CLEAR Autor: Národní úřad pro kybernetickou a informační bezpečnost, 23. 06. 2023

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) tímto doporučením reaguje na nepřehlednou situaci v oblasti TLS (SSL) doménových certifikátů určených pro webové aplikace přístupné běžné veřejnosti skrz webové prohlížeče (Google Chrome, Mozilla Firefox, Microsoft Edge a podobné).

Certifikační autority v současné době nabízí tři druhy certifikátů, které se liší mírou ověření a obvykle i cenou:

- DV (Domain Validated) – certifikační autorita pouze ověřuje, zda žadatel o certifikát má přístup k dané doméně. Obvyklé způsoby ověření jsou umístění speciálního souboru na webový server u dané domény, nastavení specifického DNS záznamu k dané doméně nebo zaslání e-mailové zprávy na určenou adresu dané domény. Cena certifikátu se pohybuje kolem 400 Kč/rok, existují ale i certifikační autority poskytující tyto certifikáty zdarma.
- OV (Organisation Validated) – probíhají ověření jako u DV certifikátu a taktéž probíhá další dodatečná ověření, jako například ověření kontaktních údajů zaslaných na e-mailovou adresu patřící k dané doméně. Cena se pohybuje kolem 3 000 Kč/rok.
- EV (Extended Validated) – probíhá ověření jako u OV certifikátu a taktéž je ověřována fyzická existence organizace telefonickým hovorem. Cena se pohybuje kolem 4 000 Kč/rok.

Výrobci prohlížečů, kteří mají největší vliv na způsobu fungování certifikačních autorit, se před několika lety rozhodli postupně utlumovat význam OV a EV certifikátů, kdy z adresního řádku zmizel název organizace uvedené v certifikátu nebo zeleně podbarvený adresní řádek v případě využití EV certifikátu. Zároveň Google Chrome od verze 106 přestal u EV certifikátů automaticky ověřovat jejich validitu pomocí protokolu OCSP.

Google navíc v březnu tohoto roku oznámil záměr omezit akceptovatelnou platnost certifikátů v Google Chrome z dnešních maximálních 398 dnů na 90 dnů. I když tato změna nebyla ještě schválena, ukazuje, jakým směrem tento výrobce nejpoužívanějšího prohlížeče uvažuje – tedy k automaticky obnovovaným certifikátům s krátkou dobou platnosti. Důvodem je nejenom fakticky nefungující revokace certifikátů, ale také obava z kvantové hrozby (možnost prolomení současných asymetrických kryptografických algoritmů pomocí kvantového počítače).

Od roku 2015 taktéž začaly vznikat certifikační autority, poskytující doménové DV certifikáty zdarma. Tyto bezplatné certifikační autority však musí splňovat stejné bezpečností pravidla, jako certifikační autority poskytující certifikáty placené – rozdíl může být v míře kvality uživatelské podpory a smluvního zajištění (např. SLA).

Z pohledu NÚKIB je pro webové aplikace přístupné veřejnosti vhodné („best practice”) využít automaticky obnovovaných certifikátů s krátkou dobou platnosti (90 dní). Automatické vystavování taktéž snižuje možnost lidské chyby při jeho vystavování a tím pádem snižuje možnost nedostupnosti systému a administrativní náklady spojené s vydáváním a změnou certifikátu. Pouze tam, kde je důvod, který jejich použití brání (není podpora na straně SW nebo HW, automatické vydávání by bylo problematické nebo tomu brání jiné právní důvody), je doporučováno využívat ručně vystavované certifikáty.

Zároveň z pohledu NÚKIB v současné době již neexistuje z bezpečnostního hlediska rozdíl mezi DV, OV nebo EV certifikáty.

Další doporučení pro vystavování a využívání doménových certifikátů

- V případě domény CZ využijte možnost požádat o zvýšení zabezpečení u registru domén CZ.NIC, aby nemohlo dojít k převzetí domény a tím i vystavení certifikátu útočníkem (https://www.nic.cz/page/4110/zadosti/)
- Vždy využijte zabezpečení DNS záznamů pomocí DNSSEC, aby nemohlo dojít k podvržení DNS záznamu při vystavovaní certifikátu certifikační autoritou (nevyužití DNSSEC může být u regulovaných organizací ze strany NÚKIB považováno za nedostatečné plnění požadavku § 25 odst. 2 písm. a) vyhlášky č. 82/2018 Sb. o o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)).
- Je také zapotřebí přihlížet k doporučení vydané NÚKIB a nasadit aktuálně odolné kryptografické algoritmy a klíče (např. využívejte pouze certifikační autority, které využívají pouze certifikáty s velikostí RSA klíče 3072 bitů a vyšší nebo certifikáty využívající eliptické křivky) – více na https://portal.neweb.govcert.cz/informacni-servis/aktuality/rsa-2048-a-dalsi-kryptograficke-algoritmy-letos-doslouzi-jste-pripraveni
- V případě pořizování nových informačních systémů nebo technologií, které mají využívat doménový certifikát, vyžadujete podporu protokolu ACME (RFC 8555) pro možnost automatického získávání a obnovování certifikátů.
- U kritických systémů buďte připraveni na situaci nutnosti změny certifikační autority v případě výpadku nebo ukončení činnosti certifikační autority.

- Certifikáty obnovujte (ať už automaticky anebo ručně) nejpozději měsíc před koncem platnosti.
- Využijte automatický monitoring konce platnosti certifikátu, pokud na živém systému má již jen 3 týdny do vypršení platnosti.
- Pokud možno nepoužívejte wildcard („hvězdičkové“) certifikáty. Tam, kde jsou opravdu potřeba, tak je nasazovat až na domény 3. úrovně. Pokud ani to nelze a je wildcard potřeba na významnou doménu 2. úrovně, mělo by vystavení tohoto certifikátu podléhat schválení osobou zodpovědnou za IT bezpečnost v dané organizaci. Tam, kde není schválena výjimka, jejich vystavování by mělo být zakázáno CAA záznamem.
- Mějte nastaveny DNS CAA záznamy (RFC 8659), které umožňují vydat certifikát pro doménu pouze uvedeným certifikačním autoritám a umožňují zablokovat vystavování wildcard certifikátu

Zdroje

Tato doporučení byla vytvořena ve spolupráci s CZ.NIC.

0