Technický standard připojení do sítí deklarantů
verze 1.1.
23/04/2019

Technický standard vychází z požadavků na škálovatelnost přístupu, kterou se rozumí schopnost v případě potřeby pružně reagovat na náhlé změny, včetně těch zásadních, dále na snadnou implementaci a také z požadavků na bezpečný přístup. Ten je definován zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „zákon o kybernetické bezpečnosti“), a vyhláškou č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „vyhláška o kybernetické bezpečnosti“).

Standard přímého přístupu do sítě (elektronického informačního systému; dále jen „IS“) deklaranta souvisí s praktickým prováděním zjednodušeného postupu „zápis do záznamů deklaranta“, v současné době primárně ve formě, zahrnující upuštění od povinnosti předkládat zboží“. Podmínky tohoto zjednodušení jsou stanoveny zejména v článku 182 nařízení Evropského parlamentu a Rady (EU) č. 952/2013, kterým se stanoví celní kodex Unie, v platném znění (dále jen „UCC“), čl. 150 nařízení Komise v přenesené pravomoci (EU) 2015/2446, kterým se doplňuje nařízení Evropského parlamentu a Rady (EU) č. 952/2013, pokud jde o podrobná pravidla k některým ustanovením celního kodexu Unie, v platném znění (dále jen „DA“) a čl. 233 až 236 prováděcího nařízení Komise (EU) 2015/2447, kterým se stanoví prováděcí pravidla k některým ustanovením nařízení Evropského parlamentu a Rady (EU) č. 952/2013, kterým se stanoví celní kodex Unie, v platném znění (dále jen „IA“). Standard je následující:

1. IS deklaranta musí být přístupný jedním z následujících způsobů:

a) Přímo dostupný ze sítě Celní správy České republiky (dále jen „CS“) zabezpečeným spojením (viz specifikace níže) přes síť Internet. Zabezpečené spojení bude sestaveno pomocí připojení webového prohlížeče klienta v síti CS k IS deklaranta. Přístup k IS deklaranta je možné omezit pomocí bezpečnostního pravidla, které přístup omezí na zdrojový adresní prostor 193.179.220.0/22, přidělený CS společností RIPE NCC.

b) Dostupný zabezpečeným spojením (viz specifikace níže) přes síť Internet, prostřednictvím webového portálu VPN koncentrátoru deklaranta. Zabezpečené spojení mezi klientem v síti CS a VPN koncentrátorem deklaranta bude sestaveno pomocí webového prohlížeče.

2. Data deklaranta musí být plnohodnotně přístupná webovým prohlížečem (Internet Explorer, Edge, Firefox, Chrome) bez nutnosti instalací jakýchkoliv klientských aplikací nebo rozšíření prohlížečů, jako je Java, Silverlight, ActiveX, FlashPlayer a jiné. Rozhraní musí být založeno pouze na bázi standardu HTML5.

3. Autentizace může být řešena:

a) Autentizace uživatelským jménem a heslem. Heslo k uživatelskému účtu musí být řízeno v souladu s požadavky zákona o kybernetické bezpečnosti, viz specifikace níže. V případě jeho vypršení musí být jasně definovaný způsob jeho obnovy. Deklarant musí v tomto modelu zpřístupnit klientům ze sítě CS i nástroj pro bezpečnou změnu hesla. Na něj jsou kladeny stejné požadavky jako na deklarantský IS.

b) Autentizace jednorázovým OTP heslem. Možná jsou jak OTP hesla generovaná specializovaným HW tokenem, tak i mobilním tokenem, tj. aplikací pro mobilní telefony. Aplikace musí být dostupná pro operační systém Android verze 8 a vyšší. Oba

typy OTP tokenů musí být v užívání CS po dobu existence přístupu. V případě mobilního OTP tokenu je nutné, aby byl deklarant ochoten mobilní aplikaci aktivovat na mobilním telefonu ve správě a majetku CS nebo aby předal inicializovanou aplikaci včetně kompatibilního mobilního telefonu CS. Pro případ reinstalace mobilního OTP tokenu musí být přesně popsán proces jeho reinicializace.

c) V rámci zajištění přístupu klientů ze sítě CS do IS deklarantů je možné využít i kombinaci obou typů autentizace a to např. tak, že OTP systém umožní přístup na VPN koncentrátor deklaranta a autentizace k IS deklaranta bude zajištěna uživatelským jménem a heslem.

4. Deklarant musí umožnit současné vícenásobné připojení klientů ze sítě CS pod stejnou identitou. CS zajistí interním procesem řízený přístup k přihlašovacím údajům a bude monitorovat spojení směrem k IS deklaranta.

5. Deklarant musí zajistit, aby klientům v síti CS nebyly zpřístupněny jiné interní IS, než právě a jedině IS „o zápisu do záznamu deklaranta v rozsahu stanoveném v UCC, DA a IA“ v režimu pouze pro čtení a případně nástroj pro změnu hesla.

6. Vlastnictví výše uvedeného adresního prostoru 193.179.220.0/22 lze ověřit zde:

https://apps.db.ripe.net/db-web-ui/#/query?searchtext=193.179.220.0%2F22#resultsSection

7. Parametry pro uživatelský účet specifikuje příloha č. 3 vyhlášky o kybernetické bezpečnosti „Minimální požadavky na kryptografické algoritmy“:

a) minimální délku hesla dvanáct znaků,

b) minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků

i. nejméně jedno velké písmeno,

ii. nejméně jedno malé písmeno,

iii. nejméně jednu číslici, nebo

iv. nejméně jeden speciální znak odlišný od požadavků uvedených v bodech i. až iii.,

v. maximální dobu pro povinnou výměnu hesla nepřesahující stoosmdesát dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.

8. Je nezbytně nutné prosazovat bezpečné nakládání s kryptografickými prostředky a zohledňovat doporučení vydaná NÚKIB a zveřejněná na jeho internetových stránkách.

Digitálně podepsáno
Mgr. Tomáš Sikora
23.04.2019 13:23:28