Bezpečnostní požadavky na AIS pro připojení k základním registrům

Verze 1.13

1. **Evidence a identifikace uživatelů AIS**.

Správce AIS musí být schopný určit, kdo požádal AIS o volání eGON služby. Iniciátorem volání může být nějaký uživatel (fyzická osoba), nebo AIS z vlastní iniciativy (např. u automaticky spouštěné úlohy). Každý AIS musí požadovat identifikaci (uživatelské jméno) při začátku práce uživatele s AIS.

2. **Obsazení agendových rolí**.

Role se vztahuje ke konkrétní činnosti v konkrétní agendě a znamená jednoznačné definování oprávnění konkrétního uživatele (fyzické osoby) při výkonu působnosti organizace (která AIS používá) v agendě. Pro každý AIS musí jeho správce zajistit vedení záznamů o tom, jaké konkrétní fyzické osoby a v jakém čase mohly vykonávat jednotlivé agendové role. A AIS musí povolit pro konkrétního uživatele pouze volání takových služeb základních registrů, ke kterým má oprávnění.

3. **Autentizace uživatelů AIS**.

Správce AIS musí zajistit autentizaci uživatele, než je mu povolena práce s AIS. Správce AIS musí zajistit poučení uživatelů o povinnosti chránit své autentizační údaje a prostředky.

4. **Zajištění bezpečnosti soukromého klíče používaného pro přístup k základním registrům**.

Soukromé klíče a certifikáty se instalují na počítače, ze kterých AIS se základními registry komunikuje. Při používání soukromého klíče a certifikátu je nutné dodržovat Certifikační politiku SZR, která je k dispozici na webových stránkách SZR www.szrcr.cz, a zajistit důvěrnost hesla pro komunikaci se SZR, pokud má správce AIS takové heslo sjednáno.

5. **Protokolování činnosti AIS**.

Správce AIS musí zajistit vytváření záznamů o činnosti AIS ve vztahu k základním registrům, minimálně:

- úspěšné přihlášení uživatele do AIS - minimálně musí obsahovat identifikaci uživatele, čas přihlášení, identifikaci zařízení, ze kterého se přihlásil,
- volání služeb základních registrů včetně parametrů.

Správce AIS musí být schopen na vyžádání SZR nebo jiného oprávněného subjektu předložit záznamy o činnosti AIS.

6. **Nahlášení narušení bezpečnosti AIS na Service Desk SZR**.

Správce AIS je povinen nahlásit zejména následujících události:

- Zneužití AIS neoprávněnou osobou s dopadem na data nebo činnost základních registrů.
- Ztráta nebo prozrazení soukromého klíče používaného AIS pro přístup k základním registrům.
- Ovlivnění AIS škodlivým kódem, tj. napadení virem apod. s dopadem na data nebo činnost základních registrů.
- Únik dat ze základních registrů.

Správce AIS je povinen seznámit uživatele AIS s povinností hlásit bezpečnostní události buď přímo na Service Desk SZR, nebo přes správce AIS.

7. **Nahlášení podezření na narušení bezpečnosti základních registrů na Service Desk SZR**.

Správce AIS je povinen nahlásit zejména následujících události:

- Není dostupná aplikační služba základních registrů, která byla dříve dostupná.
- Chybí data základních registrů, o kterých uživatel ví, že by měla být dostupná.

Správce AIS je povinen seznámit uživatele AIS s povinností hlásit narušení bezpečnosti základních registrů buď přímo na Service Desk SZR, nebo přes správce AIS.

8. Použití dostatečně silných kryptografických prostředků pro komunikaci mezi AIS a ISZR.

Komunikace mezi AIS a ISZR (Informační systém základních registrů) probíhá vždy protokolem https (http over SSL), tedy šifrovaně. To je vynuceno na straně ISZR, ať ISZR vystupuje z hlediska navazování spojení v roli klienta nebo serveru. ISZR vyžaduje určitou kvalitu parametrů SSL, popis je v dokumentu "Konfigurace SSL pro připojení AIS k ISZR" na webu SZR.

AIS musí být nakonfigurován tak, aby mohl uvedené parametry akceptovat. Tyto parametry se mohou měnit.

9. **AIS musí autentizovat ISZR s využitím certifikátu ISZR**.

Pokud navazuje spojení AIS, nabízí mu ISZR svůj certifikát automaticky. Pokud navazuje spojení ISZR, musí ho AIS o jeho certifikát požádat v rámci navazování SSL spojení a ISZR mu ho poskytne.

AIS musí certifikát zkontrolovat, že byl vydán pro ISZR a že je platný.

Tento požadavek je upřesněním a zdůrazněním povinnosti spoléhající se strany ověřit identitu druhé strany uvedené v Certifikační politice SZR (kap. 1.3.4). Údaje o certifikátech ISZR jsou uveřejněny na webu SZR v dokumentu „Certifikáty a jejich použití“.

10. **V žádostech o připojení AIS k základním registrům uvádět pouze IP adresy, které je správce AIS oprávněn používat**.

Správce AIS je odpovědný za to, že jím spravovaný AIS nepoužívá neoprávněně nějaké IP adresy, které poskytovatel připojení (k síti Internet nebo k síti KIVS) poskytl jinému subjektu. A správce AIS je odpovědný za to, že tyto adresy uvedl správně v žádosti o připojení AIS k základním registrům.

11. **Zajistit, že AIS nepoužívají ke komunikaci se základními registry IP adresy jiného správce**.

Není povoleno, aby AIS se dvěma různými správci používaly pro komunikaci se základními registry stejné IP adresy. Platí to pro IP adresy pro volání synchronních i asynchronních eGON služeb i pro adresy pro doručování odpovědí na asynchronní služby v aktivním režimu.

Platí jednotně pro všechny IP adresy, ať už použité v testovacím anebo produkčním prostředí základních registrů.

12. **Nastavení správného systémového času na počítačích AIS**.

Správce AIS je odpovědný za nastavení správného systémového času na počítačích, na kterých je AIS provozovaný včetně těch, které komunikují se základními registry. Důvodem je požadavek na průkaznost záznamů o činnosti AIS a správné ověřování platnosti certifikátů. SZR doporučuje synchronizovat systémový čas serverů komunikujících se základními registry s nějakým spolehlivým zdrojem času, například s NTP servery Centrálního místa služeb.

13. **Zajištění bezpečnosti počítačů AIS**.

Správce AIS musí zajistit omezení přístupu k počítačům, na kterých je AIS provozován včetně těch, ze kterých AIS komunikuje se základními registry (např. počítače komunikační sběrnice). Počítače nesmí být volně přístupné. Musí být zajištěna instalace bezpečnostních aktualizací operačního systému počítačů. Musí být zajištěno vymazání údajů ze základních registrů a údajů umožňujících přístup k základním registrům na počítačích, pokud přestanou být pro provoz AIS používány.

Správce AIS musí zajistit bezpečné prostředí pro provoz AIS. Bezpečné prostředí zahrnuje bezpečný DNS, bezpečnou konfiguraci směrování (routing), bezpečnost bran, proxy serverů a podobných zařízení.

14. **V případě, že SZR zjistí, že AIS ohrožuje bezpečnost základních registrů, má SZR právo mu až do doby vyřešení problému zablokovat přístup k základním registrům**.

SZR monitoruje činnost AIS při práci se základními registry a sleduje pokusy o narušení bezpečnosti. Ty mohou mít různou podobu, ale zejména se jedná o opakovaná neautorizovaná volání služeb a o pokusy o zahlcení systému základních registrů požadavky na služby ze strany AIS. V případě, že SZR pokus o narušení bezpečnosti základních registrů zjistí, pokusí se vyjasnit a vyřešit událost se správcem AIS. SZR může v nezbytném případě, nebo pokud se nepodaří událost vyřešit, zablokovat přístup AIS k ISZR. Může blokovat přístup s použitím certifikátů přidělených AIS, nebo může blokovat přístup z IP adres, které AIS používá. Jde pouze o dočasné zablokování přístupu k základním registrům. V případě blokování certifikátů nejde o zneplatnění certifikátu, respektive certifikátů, který

byl, respektive které byly pro AIS přiděleny. SZR bude zablokování přístupu AIS provádět pouze v případě závažných pokusů o narušení bezpečnosti základních registrů.

SZR **doporučuje**, aby správce AIS realizoval i následující opatření.

1. **Filtrovat provoz mezi AIS a ISZR**.

Omezit komunikaci s ISZR na seznam IP adres patřících ISZR. AIS nebo jeho firewall zkontroluje IP adresu, ze které je navazováno spojení s AIS, respektive zkontroluje IP adresu, na kterou AIS navazuje spojení, a povolí komunikaci pouze s ověřenou adresou ISZR.

2. **Používat pro jednotlivé AIS různé IP adresy**.

SZR doporučuje používat pro jednotlivé AIS různé IP adresy, aby byl provoz jednotlivých AIS identifikovatelný a oddělitelný na síťové vrstvě. Umožní to jemnější diagnostiku a rychlejší a přesnější řešení problémů.

3. **Používat v produkčním a testovacím prostředí různé IP adresy**.

SZR doporučuje používat v produkčním a testovacím prostředí různé IP adresy, aby byl provoz pro produkční a testovací prostředí oddělen již na síťové vrstvě. Nároky na bezpečnost jsou v každém prostředí různé a problémy způsobené nějakým AIS v testovacím prostředí mohou ovlivnit i dostupnost AIS v produkčním prostředí, pokud AIS používá v obou prostředích stejné IP adresy.

4. **Minimalizovat počet počítačů se soukromými klíči a certifikáty**.

SZR doporučuje minimalizovat počet počítačů, na které se instalují soukromé klíče a certifikáty pro přístup do základních registrů.