Digitální a informační agentura

Bezpečnostní požadavky na AIS/SSVÚ pro připojení k základním registrům a k ISSS

Verze 2.1

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

Správce AIS/SSVÚ (Agendový informační systém / Soukromoprávní systém pro využívání údajů) musí být schopný určit, kdo požádal AIS/SSVÚ o volání služby základních registrů anebo ISSS (Informační systém sdílené služby). Iniciátorem volání může být nějaký uživatel (fyzická osoba), nebo AIS/SSVÚ z vlastní iniciativy (např. u automaticky spouštěné úlohy). Každý AIS/SSVÚ musí požadovat identifikaci (uživatelské jméno) při začátku práce uživatele s AIS/SSVÚ.

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 v agendě. Pro každý AIS/SSVÚ musí jeho správce zajistit vedení záznamů o tom, jaké konkrétní fyzické osoby a v jakém čase mohly vykonávat jednotlivé agendové role. A AIS/SSVÚ musí povolit pro konkrétního uživatele pouze volání takových služeb základních registrů a ISSS, ke kterým má oprávnění.

3. **Autentizace uživatelů AIS/SSVÚ**.

Správce AIS/SSVÚ musí zajistit autentizaci uživatele, než je mu povolena práce s AIS/SSVÚ. Správce AIS/SSVÚ 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/SSVÚ se základními registry a s ISSS komunikuje. Při používání soukromého klíče a certifikátu je nutné dodržovat Certifikační politiku DIA pro certifikáty vydávané pro AIS (dále jen Certifikační politika), která je k dispozici na webu DIA (www.szrcr.cz), a zajistit důvěrnost hesla pro komunikaci s DIA, pokud má správce AIS/SSVÚ takové heslo sjednáno.

5. **Protokolování činnosti AIS/SSVÚ**.

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

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

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

6. **Nahlášení narušení bezpečnosti AIS/SSVÚ na Service Desk DIA**.

Správce AIS/SSVÚ je povinen nahlásit zejména následujících událostí:

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

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

7. **Nahlášení podezření na narušení bezpečnosti základních registrů anebo ISSS na Service Desk DIA**.

Správce AIS/SSVÚ je povinen nahlásit zejména následujících událostí:

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

Správce AIS/SSVÚ je povinen seznámit uživatele AIS/SSVÚ s povinností hlásit narušení bezpečnosti základních registrů a ISSS buď přímo na Service Desk DIA, nebo přes správce AIS/SSVÚ.

8. **Použití dostatečně silných kryptografických prostředků pro komunikaci mezi AIS/SSVÚ a ISZR / ISSS**.

Komunikace mezi AIS/SSVÚ a ISZR (Informační systém základních registrů) i mezi AIS/SSVÚ a ISSS (Informační systém sdílené služby) probíhá vždy protokolem https (http over SSL), tedy šifrovaně. To je vynuceno na straně ISZR / ISSS, ať ISZR / ISSS vystupuje z hlediska navazování spojení v roli klienta nebo serveru. AIS/SSVÚ musí být nakonfigurován tak, aby mohl příslušné parametry akceptovat. Tyto parametry se mohou měnit.

9. **AIS/SSVÚ musí autentizovat ISZR a ISSS**.

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

AIS/SSVÚ musí certifikát zkontrolovat, že byl vydaný pro ISZR, respektive pro ISSS a že je platný.

Tento požadavek je upřesněním a zdůrazněním povinnosti spoléhající se strany ověřit identitu druhé strany uvedené v Certifikační politice.

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

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

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

Není povoleno, aby AIS/SSVÚ se dvěma různými správci používaly pro komunikaci se základními registry stejné IP adresy. Platí to pro IP adresy pro volání synchronních i asynchronních služeb základních registrů a ISSS 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 nebo ISSS.

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

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

13. **Zajištění bezpečnosti počítačů AIS/SSVÚ**.

Správce AIS/SSVÚ musí zajistit omezení přístupu k počítačům, na kterých je AIS/SSVÚ provozovaný včetně těch, ze kterých AIS/SSVÚ komunikuje se základními registry anebo s ISSS (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 a k ISSS na počítačích, pokud přestanou být pro provoz AIS/SSVÚ používány.

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

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

DIA monitoruje činnost AIS/SSVÚ při práci se základními registry a s ISSS 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/SSVÚ. V případě, že DIA pokus o narušení bezpečnosti základních registrů anebo ISSS zjistí, pokusí se vyjasnit a vyřešit událost se správcem AIS/SSVÚ. DIA může v nezbytném případě, nebo pokud se nepodaří událost vyřešit, zablokovat přístup AIS/SSVÚ k základním registrům anebo k ISSS. Může blokovat přístup s použitím certifikátů přidělených AIS/SSVÚ, nebo může blokovat přístup z IP adres, které AIS/SSVÚ používá. Jde pouze o dočasné zablokování přístupu k základním registrům anebo k ISSS. V případě blokování certifikátů nejde o zneplatnění certifikátu, respektive certifikátů, který byl, respektive které byly pro AIS/SSVÚ přiděleny. DIA bude zablokování přístupu AIS/SSVÚ provádět pouze v případě závažných pokusů o narušení bezpečnosti základních registrů.

DIA **doporučuje**, aby správce AIS/SSVÚ realizoval i následující opatření.

1. **Filtrovat provoz mezi AIS/SSVÚ a ISZR/ISSS**.

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

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

DIA doporučuje používat pro jednotlivé AIS/SSVÚ různé IP adresy, aby byl provoz jednotlivých AIS/SSVÚ 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**.

DIA doporučuje používat v produkčním a testovacím prostředí základních registrů a ISSS 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/SSVÚ v testovacím prostředí mohou ovlivnit i dostupnost AIS/SSVÚ v produkčním prostředí, pokud AIS/SSVÚ používá v obou prostředích stejné IP adresy.

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

DIA doporučuje minimalizovat počet zařízení (servery, komunikační sběrnice, SSL koncentrátory, firewally apod.), na které se instalují soukromé klíče a certifikáty pro přístup do základních registrů a do ISSS.