

Výklad k § 6 písm. c) vyhlášky č. 366/2001 Sb.

Ověření bezpečnosti informačního systému pro certifikační služby z hlediska požadavků § 6 písm. c) vyhlášky č. 366/2001 Sb.

Dokument je určen všem poskytovatelům certifikačních služeb, kteří vydávají nebo uvažují o vydávání kvalifikovaných certifikátů.

Obsah

Výklad k § 6 písm. c) vyhlášky č. 366/2001 Sb.

Ověření bezpečnosti informačního systému pro certifikační služby z hlediska požadavků
§ 6 písm. c) vyhlášky č. 366/2001 Sb.

Obsah	2
1 Úvod do problematiky	3
2 Komentář a výklad	3
2.1 Kontrola bezpečnostní shody.....	3
2.2 Dokumentace systému	5
3 Použité zkratky.....	7
4 Literatura	7

1 Úvod do problematiky

Podle § 6 písm. c) vyhlášky č. 366/2001 Sb. je jedním z požadavků ověření bezpečnosti používání informačního systému pro certifikační služby a zajištění dostatečné bezpečnosti postupů, které tento systém podporují, doložení:

„písemného posudku, jehož součástí je potvrzení, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti, [1] je používání informačního systému pro certifikační služby v souladu se způsoby zajištění bezpečnosti stanovenými v dokumentech uvedených v § 2 odst. 1 písm. c) a d). Kontrola bezpečnostní shody musí být prováděna opakovaně, a to vždy nejpozději do 12 měsíců od provedení poslední kontroly bezpečnostní shody“.

Základní požadavky na bezpečnost jsou specifikovány v zákoně č. 227/2000 Sb. a precizovány vyhláškou č. 366/2001 Sb.; v souladu s ustanovením § 2 odst. 7 jsou Odborem elektronického podpisu zveřejňována další upřesnění.

Odbor elektronického podpisu specifikoval, že při zpracování celkové bezpečnostní politiky (dále jen „CBP“) a systémové bezpečnostní politiky (dále jen „SBP“) se postupuje podle norem:

- ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT (dále jen „ČSN 13335“) 1–3,
- ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti (dále jen „ČSN 17799“).

2 Komentář a výklad

2.1 Kontrola bezpečnostní shody

Kontrola bezpečnostní shody [2] může být použita (ČSN 13335-3, kap. 11.2) ke kontrole shody:

- nových systémů a služeb IT po jejich implementaci (odsouhlasení – ČSN 13335-3, kap. 10.4),
- existujících systémů a služeb IT (monitorování, řešení incidentů – ČSN 13335-3, kap. 11.5),
- existujících systémů a služeb IT, když byly provedeny změny dotýkající se bezpečnosti systému IT (řízení změn – ČSN 13335-3, kap. 11.3).

Cílem kontroly bezpečnostní shody (ČSN 13335-3, kap. 11.2) je získat ujištění, že ochranná opatření

- jsou implementována,
- jsou implementována správně,
- jsou správně používána,
- jsou testována tehdy, je-li to důležité,
- poskytují vhodnou úroveň ochrany (v případě odsouhlasení se jedná o explicitní požadavek na ujištění).

Předmětem kontroly bezpečnostní shody jsou ochranná opatření jak u vlastních informačních technologií, tak i technologií obchodních partnerů, resp. poskytovatelů systémů (ČSN 13335-3, kap. 10.4; ČSN 17799, kap. 12.2.1).

Z hlediska efektivnosti je podstatné (ČSN 13335-2, kap. 16.2), aby ochranná opatření byla a zůstala ve shodě se specifikovanými ochrannými opatřeními (viz bezpečnostní politiky; plán bezpečnosti systému (ČSN 13335-2, kap. 13; ČSN 13335-3, kap. 9.7)) v průběhu

- akvizice
- vývoje
- provozu
- údržby (včetně ukončení provozu/vyřazení z provozu).

Terminologie a členění životního cyklu vychází ze standardu ISVS [3] (dále jen „S_1_5“). Hlavním důvodem jeho užití je sjednocení metodiky a terminologie. Tento standard je veřejně dostupný, integruje v sobě i problematiku bezpečnosti, je zpracován v souladu s ČSN ISO/IEC 12207 a případnému zájemci může poskytnout doplňující informace.

2.1.1 Personál provádějící kontrolu bezpečnostní shody

Kontrolu bezpečnostní shody mohou provádět externí nebo interní pracovníci (ČSN 13335-2, kap. 16.2; ČSN 13335-3, kap. 11.2). V souladu s dokumenty CWA 14172-3:2001 (E) [4] kap. 3.5 lze doporučit, aby vedle odborné kompetentnosti byla prokázána i nezávislost subjektu provádějícího kontrolu bezpečnostní shody; z ČSN 13335-2 kap. 9.2. lze dovodit odpovědnost statutárního orgánu za specifikaci požadavků na kvalitu a kompetence subjektů provádějících kontrolu bezpečnostní shody.

2.1.2 Realizační výstupy kontroly bezpečnostní shody; posudek, potvrzení

Postupy či forma a obsah realizačních výstupů kontroly bezpečnostní shody nejsou vyhláškou ani zmíněnými normami exaktně specifikovány (interními normami organizace je možné navíc zohlednit i další potřeby, např. prioritu efektivnosti); norma (ČSN 13335-3, kap. 10.4) explicitně předpokládá přizpůsobení konkrétnímu systému IT.

Z hlediska postupů norma uvádí, že se jedná zejména o revize dokumentů, fyzické inspekce a technická hodnocení. Z normou specifikovaných klíčových činností (např. ČSN 13335-3, kap. 10.4 a 11.1; ČSN 17799, kap. 12), určení (ČSN 13335-2, kap. 16.3 a 7.2) a principů integrity lze dovodit, že realizačním výstupem budou minimálně:

- zpráva (ve vyhlášce č. 366/2001 Sb. nazývána „posudek“) popisující průběh kontroly bezpečnostní shody, prezentující postupy, požadavky, použité a zjištěná fakta a závěry (zejména ve vztahu k normou explicitně specifikovaným klíčovým problémům – např. ČSN 13335-3, kap. 10.4, 11.2, 11.4), a to vše takovým způsobem, aby jiný čtenář zprávy (předpokládá se, že je obeznámen s obecnými principy bezpečnosti) mohl snadno nalézt informace, jež ho zajímají;

a

- hlášení (ve vyhlášce č. 366/2001 Sb. nazýváno „potvrzení“)
 - shrnující závěry z procesu kontroly bezpečnostní shody
 - a konstatující zejména:
 - zda bezpečnost byla odsouhlasena „plně“, „částečně“, „s omezením“, či odsouhlasena „nebyla“;
 - zda existují doklady o zřeknutí se práva na bezpečnost a zda trvá jejich platnost;
 - zda existují jakákoli omezení zpracování;
 - za jakých podmínek (změny systému nebo jeho okolí; platnost hodnocení; periodicita) by se měla opakovat kontrola bezpečnostní shody.

Realizační výstupy pak slouží jako podklad k udělení souhlasu (ČSN 13335-2, kap. 14) s uvedením systému nebo služby do provozu (resp. pokračováním v provozu); primárně tento souhlas uděluje management organizace.

2.2 Dokumentace systému

Jedním z atributů dokumentace systému je i lokace v čase, resp. místo a určení v životním cyklu.

Celková bezpečnostní politika („CBP“) a systémová bezpečnostní politika („SBP“) vznikají v počátečních fázích životního cyklu systému.

Certifikační prováděcí směrnice, plán pro zvládání krizových situací a plán obnovy tvoří součást výstupů vývojové etapy; jsou v nich popsány způsoby zajištění cílů z CBP a SBP.

Požadavek § 6 písm. c) vyhlášky č. 366/2001 Sb. explicitně odkazuje na CBP a SBP; z principů kontroly bezpečnostní shody dovedeme významnost výstupů, zejména pak certifikační prováděcí směrnice, plánu pro zvládání krizových situací a plánu obnovy. S vědomím této skutečnosti vyhláška č. 366/2001 Sb. § 2 odst. 1 vyžaduje po poskytovateli certifikačních služeb doložení i těchto dokumentů.

2.2.1 Celková bezpečnostní politika

CBP je dokumentem strategického významu; v organizaci každému známý dokument (ČSN 13335-3, kap. 10.2; ČSN 17799, kap. 3), vytvářející základ pro dosažení a udržení specifikované úrovně bezpečnosti.

Forma a stupeň podrobnosti CBP nejsou normami exaktně specifikovány; z požadavků norem (ČSN 13335-3, kap. 7.2; ČSN 17799, kap. 3) lze dovést, že musí splňovat zejména předpoklady úplnosti, srozumitelnosti, měřitelnosti, odpovědnosti, vynutitelnosti a vymahatelnosti.

Z hlediska obsahu Odbor elektronického podpisu (dále **OEP**) doporučuje využít generická návěští kapitol, resp. podkapitol ČSN 13335-3, příloha A a ČSN 17799.

K omezení zneužitelnosti informací obsažených v CBP OEP doporučuje, aby základní dokument, určený všem zaměstnancům i uživatelům, obsahoval přílohy s problémově orientovaným obsahem a selektivní dostupností; to však nikoli na úkor integrity.

Podstatné je, aby CBP specifikovala bezpečnostní cíle vyplývající z:

- charakteru činnosti organizace a jejího poslání,
- požadavků (případně omezení) managementu,
- legislativního prostředí a regulačních závazků,
- bezpečnosti obecně.

Významným cílem, zejména pro poskytovatele certifikačních služeb, je i stanovení požadované míry bezpečnosti a úrovně její zaručitelnosti.

Na základě hrubé analýzy rizik jsou definovány priority a doporučeny prostředky k dosažení cílů, vymezeny zdroje a určena přijatelná zbytková rizika.

S ohledem na to, že nelze vyloučit poskytování některých služeb externími subjekty, považuje OEP za významné, aby již na této úrovni byly vytvořeny předpoklady pro adekvátní naplnění legislativních požadavků v procesu kontroly bezpečnostní shody.

CBP je chápána jako dokument střednědobé platnosti; revize či vyšší míra podrobnosti CBP může být vyvolána změnami analýzy rizik, manažerskou revizí, výsledky kontroly bezpečnostní shody či vyhodnocením bezpečnostních incidentů.

Dalšími procesy je CBP rozpracována do vyšší míry podrobnosti a konkretizace v odpovídajících systémových bezpečnostních politikách.

2.2.2 Systémová bezpečnostní politika informačního systému

SBP vzniká v počátečních fázích životního cyklu systému a navazují na ni plány systému a dokumentace k testům (ČSN 13335-3, kap. 9.6 a 9.7; S_1_5 – kap. 6.3. a 7.13).

Forma a obsah SBP nejsou normami exaktně specifikovány; účelem SBP je specifikovat či řešit úkoly na vyšší úrovni podrobnosti a s vyšší mírou poznání, než je tomu u CBP. Klíčové statě SBP

jsou uvedeny v ČSN 13335-2, kap. 12 a ČSN 13335-3, kap. 9.6.; požadavek na popis vazeb na okolní informační systémy (vyhláška č. 366/2001 § 2 odst. 6 písm. b)) lze naplnit i formou bezpečnostních politik rozhraní.

SBP je schvalována vyšším managementem organizace jako závazný soubor zásad a pravidel; s ohledem na návaznost alokace adekvátních zdrojů (vazba na plán bezpečnosti systému) k implementaci a prosazování bezpečnosti v provozu je nezbytné, aby údaje uvedené v SBP vycházely z úplného výčtu, byly konkrétní a identifikovaly ochranná opatření pro dosažení požadované míry bezpečnosti a úrovně zaručitelnosti (vazba na dokumentaci k testům).

Odbor elektronického podpisu považuje za podstatné zdůraznit požadavek zohlednit v analýze rizik nejen bezpečnost obecně, ale věnovat odpovídající pozornost specifickým atributům systému, organizace a jejího okolí.

2.2.3 Plán pro zvládání krizových situací a plán obnovy

Řízení kontinuity podnikatelských činností se věnuje kapitola 11 ČSN 17799, zatímco norma ČSN 13335 nevyčleňuje tyto aktivity, ale předpokládá, že se jedná o naplnění cílů CBP a SBP (existenci plánů lze dovodit např. z činností při řešení incidentů – ČSN 13335-2, kap. 16.4 a ČSN 13335-3, kap. 11.5.); cíle, analýza rizik a plán bezpečnosti primárně určují inherentní robustnost systému, z které je odvozen charakter plánu pro zvládání krizových situací a plán obnovy (dále jen „PKSPO“).

Forma a obsah PKSPO nejsou normami exaktně specifikována; účelem PKSPO je, aby činnost organizace mohla být obnovena v požadovaných lhůtách, resp. byl vytvořen předpoklad k minimalizaci škod. OEP předpokládá, že generické činnosti uvedené v ČSN 17799, kap. 11 budou rozpracovány do konkrétních podmínek systému; současně je připraven akceptovat, aby forma byla podřízena účelu PKSPO.

OEP přikládá vysoký význam testování, udržování a přehodnocování PKSPO.

2.2.4 Certifikační prováděcí směrnice

Citované normy ČSN 13335 a ČSN 17799 mají vyšší míru obecnosti a širší aplikovatelnosti. Problematické kryptografických opatření je explicitně věnována kapitola 10.3 ČSN 17799.

Vyhláška č. 366/2001 Sb. v § 2 odst. 4 uvádí, že:

„obsahem certifikační prováděcí směrnice je zejména stanovení postupů, které poskytovatel certifikačních služeb vydávající kvalifikované certifikáty uplatňuje při zajištění služeb spojených s elektronickými podpisy.“

Forma a obsah certifikační prováděcí směrnice (dále jen „CPS“) nejsou výše uvedenými normami exaktně specifikovány. OEP doporučuje, aby pro CPS byla použita struktura uvedená v RFC 2527.

Na bázi RFC 2527 byl OEP zpracován dokument, který extrahuje podstatné ve vztahu ke struktuře CPS. Dokument, v jazyce českém, bude na vyžádání zaslán zájemcům elektronickou poštou. Žádosti lze uplatnit na adrese elektronické podatelny ministerstva informatiky: **posta@micr.cz**.

S ohledem na význam CPS a její postavení ve vztahu k CBP, SBP, PKSPO a směrnícím systému považuje OEP za optimální, aby CPS v jednotlivých kapitolách a subkapitolách rekapitulovala relevantní bezpečnostní cíle, zásady a pravidla a následně specifikovala způsoby jejich naplnění, resp. stručnou charakteristiku této realizace, a odkaz na příslušné směrnice, resp. jiné interní normativy.

3 Použité zkratky

CBP	celková bezpečnostní politika
CPS	certifikační prováděcí směrnice
EESSI	European Electronic Signature Standardization Initiative
ISVS	informační systém veřejné správy
IT	informační technologie
PKSPO	plán pro zvládání krizových situací a plán obnovy
S_1_5	Standard ISVS pro náležitosti životního cyklu informačního systému verze 1.1; Věstník Úřadu pro veřejné informační systémy, ročník 1, částka 5; Praha 2000
SBP	systémová bezpečnostní politika

4 Literatura

- [1] ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1–3.
- [2] Kontrola bezpečnostní shody je nazývána také bezpečnostní audit nebo bezpečnostní revize (ČSN 13335-2, kap. 16.2.
- [3] Standard ISVS pro náležitosti životního cyklu informačního systému verze 1.1; Věstník Úřadu pro veřejné informační systémy, ročník 1, částka 5; Praha 2000.
- [4] EESSI Conformity Assessment Guidance – part 3: Trustworthy Systems Managing Certificates for Electronic Signatures.