Národní úřad
pro kybernetickou
a informační bezpečnost

P. O. BOX 17
616 00 Brno 16
www.nukib.cz

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Upozornění odboru bezpečnosti informačních a komunikačních technologií k fyzické bezpečnosti pro informační systémy

Poté, co vstoupila v platnost novela č. 19/2008 Sb. vyhlášky č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, bylo zaznamenáno několik případů určitého neporozumění postupu, jakým se stanovují opatření fyzické bezpečnosti v informačních systémech pro nakládání s utajovanými informacemi.

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor (dále jen „vyhláška č. 523/2005 Sb.“), ukládá v § 3 zajistit bezpečnost utajovaných informací v informačním systému souborem několika typů bezpečnostních opatření, ve kterém vystupuje i fyzická bezpečnost informačního systému.

Soubor bezpečnostních požadavků pro určitý informační systém se vytváří z minimálních bezpečnostních požadavků, z požadavků vyplývajících z použitého bezpečnostního provozního módu a z nejvyššího stupně utajení utajovaných informací, který může být v informačním systému zpracováván, a z **požadavků odvozených z analýzy rizik provedené pro tento informační systém** (nebo typ informačního systému).

Fyzickou bezpečností pro informační systémy se rámcově zabývá § 20 vyhlášky č. 523/2005 Sb. Podle něho se během certifikace informačního systému stanovuje, které komponenty IS musí být umístěny v zabezpečené oblasti nebo objektu a jejich kategorie.

Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb. (dále jen „vyhláška č. 528/2005 Sb.“), stanoví bodové ohodnocení jednotlivých opatření fyzické bezpečnosti a **nejnižší míru zabezpečení zabezpečené oblasti**.

Pro ochranu utajovaných informací stupně utajení Důvěrné nebo vyššího je tato nejnižší míra zabezpečení postačující zpravidla i pro informační systémy.

V případě utajovaných informací stupně utajení Vyhrazené je situace odlišná. Zatímco pro ochranu klasických papírových utajovaných dokumentů jsou minimální požadavky na zabezpečenou oblast kategorie Vyhrazené (typ 0) považovány za dostačující, pro utajované informace vyskytující se v informačním systému v elektronické podobě může z analýzy rizik vyplynout potřeba jejich zesílení.

Ke snížení rizika na úroveň akceptovatelnou pro získání certifikátu informačního systému pro stupeň utajení Vyhrazené je třeba přijmout dodatečná opatření zejména pro ochranu vyjímatelného nebo zabudovaného HDD, v případě lokálních počítačových sítí také pro jejich rozvody. O konkrétní realizaci zvýšení úrovně fyzické bezpečnosti se potom rozhoduje v rámci certifikace informačního systému, vhodné řešení se hledá s uvážením charakteru zpracovávaných utajovaných informací a se snahou o co nejnižší dodatečné náklady, s přihlédnutím k možnostem žadatele o certifikaci.

Upozorňujeme, že zabezpečené oblasti všech kategorií jsou v rámci bezpečnostní prověrky podnikatele často hodnoceny ještě bez zahrnutí možnosti, že v nich bude umístěn informační systém, který vyžaduje certifikaci.

To znamená, že

- tabulka bodového ohodnocení sestavená podle kapitoly 12 přílohy č. 1 k vyhlášce č. 528/2005 Sb., kde je použita hodnota parametru S1 (S1=SS1 x SS2) pro úschovný objekt, vyhovuje pouze pro informační systémy s vyjímatelnými HDD,
- pro informační systém se zabudovaným HDD je nutné dosáhnout potřebné výše bodového ohodnocení s použitím hodnot parametrů SS1 a SS2 podle kapitoly 13, které jsou zpravidla nižší,
- pro zpracování utajovaných informací stupně utajení Vyhrazené se může v průběhu certifikace informačního systému zabezpečená oblast kategorie Vyhrazené typu 0, tedy s nulovým bodovým ohodnocením, projevit jako nedostatečná pro informační systémy jak s vyměnitelnými, tak i zabudovanými HDD.

Během certifikace informačního systému mohou tedy vzniknout dodatečné požadavky na jeho fyzické zabezpečení.

Podnikateli, který požádal o bezpečnostní prověrku podnikatele a zamýšlí zřízení informačního systému pro nakládání s utajovanými informacemi, doporučujeme již v raném stádiu řízení k osvědčení podnikatele konzultovat s Národním úřadem pro kybernetickou a informační bezpečnost problematiku bezpečnosti informačních systémů a pro zpracování utajovaných informací stupně utajení Důvěrné nebo vyššího navíc také oblast kompromitujícího elektromagnetického vyzařování. Konzultace mohou snížit jeho náklady na vybudování informačního systému.

Rovněž doporučujeme podnikateli, aby upozornil na tuto skutečnost pracovníky odboru administrativní a fyzické bezpečnosti Národního bezpečnostního úřadu, kteří provádějí hodnocení zabezpečených oblastí a konzultovat s nimi (byť i do budoucnosti) možná řešení.