10.1 Akvizice, vývoj a údržba

Tento dokument popisuje opatření, které MUSÍ nebo BY MĚLO být implementováno pro:

- **Bezpečnostní požadavky pro akvizici, vývoj a údržbu.**
- **Řízení zranitelností.**
- **Politika poskytování a nabývání licencí programového vybavení a informací.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti – Akvizice, vývoj a údržba (§ 13).

1 Bezpečnostní požadavky pro akvizici, vývoj a údržbu

Cíl: Řízení rizik a významných změn včetně stanovení bezpečnostních požadavků do procesů akvizice, vývoje a údržby. Zvyšování kybernetické bezpečnosti již v počátečních fázích projektů. Zahrnutím bezpečnostních požadavků od počátku dochází ke snižování nákladů, které by jinak bylo nutné vynaložit na zabezpečení v průběhu používání informačních nebo komunikačních systémů, kdy tyto náklady bývají

1.1 Bezpečnostní požadavky

Společnost MUSÍ stanovit pravidla pro akvizici, vývoj a údržbu.

Implementační pokyny:

1.1.1 Společnost v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému MUSÍ řídit rizika.

1.1.2 Společnost MUSÍ řídit významné změny.

1.1.3 Společnost MUSÍ zajistit bezpečnost vývojového a testovacího prostředí nejlépe formou fyzického nebo logického oddělení od provozu.

1.1.4 Společnost MUSÍ zajistit bezpečnost testovacích dat v celém jejich životním cyklu v činnosti, při uložení a následně při archivaci těchto dat.

1.1.5 Společnost MUSÍ zajistit testování významných změn před jejich zavedením do provozu.

1.1.6 Je-li cílem provedení akvizice nebo vývoje nástroj pro správu identity, MUSÍ společnost zajistit splnění požadavků na:

- ověření identity před zahájením aktivit v informačním a komunikačním systému,
- řízení počtu možných neúspěšných pokusů o přihlášení,
- odolnost uložených nebo přenášených autentizačních údajů proti neoprávněnému odcizení a zneužití,
- ukládání autentizačních údajů ve formě odolné proti offline útokům,
- opětovné ověření identity po určené době nečinnosti,
- dodržení důvěrnosti autentizačních údajů při obnově přístupu a centralizovanou správu identit.

1.1.7 Společnost MUSÍ nastavit vynucování pravidel pro ověřování identity uživatelů, administrátorů a aplikací heslo s těmito požadavky:

- délky hesla alespoň:
  - 12 znaků u uživatelů a
  - 17 znaků u administrátorů a aplikací,
- umožňující zadat heslo o délce alespoň 64 znaků,
- neomezující použití malých a velkých písmen, číslic a speciálních znaků,
- umožňující uživatelům změnu hesla, přičemž období mezi dvěma změnami hesla nesmí být kratší než 30 minut,
- neumožňující uživatelům a administrátorům zvolit si nejčastěji používaná hesla, tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem a opětovné použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel a pro povinnou změnu hesla v intervalu maximálně po 18 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie.
- Viz směrnice SM-7 Řízení přístupu

1.1.8 Společnost MUSÍ v případě používání autentizace pouze účtem a heslem:

- vynutit bezodkladnou změnu výchozího hesla po jeho prvním použití,
- bezodkladně zneplatnit heslo sloužící k obnovení přístupu po jeho prvním použití nebo uplynutím nejvýše 60 minut od jeho vytvoření a
- povinně zahrne pravidla tvorby bezpečných hesel do plánu rozvoje bezpečnostního povědomí.

1.1.9 Společnost MUSÍ nastavit nástroj pro ověření identity uživatelů, administrátorů a aplikací, s použitím autentizace pomocí kryptografických klíčů.

1.1.10 Společnost MUSÍ využívat autentizační mechanizmus založený na principu vícefaktorové autentizace s nejméně dvěma různými typy faktorů.

1.1.11 Na základě posouzení bezpečnostních aspektů informačního nebo komunikačního systému MUSÍ správce informačního nebo komunikačního systému definovat konkrétní bezpečnostní požadavky na informační nebo komunikační systém pro zjištění důvěrnosti, dostupnosti a integrity informací v informačním nebo komunikačním systému. Požadavky musí být v souladu s existujícími směrnicemi, zejména použité bezpečnostní komunikační protokoly, způsoby a možnosti šifrování. Součástí požadavků musí být i definování komunikační matice při vývoji aplikace.

1.1.12 Správce informačního nebo komunikačního systému MUSÍ zajistit v oprávněných případech návrh splnění bezpečnostních požadavků.

1.1.13 Součástí těchto obecných požadavků MUSÍ být:

- identifikace dat vytvářených, zpracovávaných a ukládaných v informačním nebo komunikačním systému,
- definice klíčových bezpečnostních rolí včetně školení uživatelů, správců a vývojářů,
- identifikace zdrojů požadavků na informační nebo komunikační systém z hlediska bezpečnosti a regulatorních požadavků.

1.1.14 V případě vyvíjeného informačního nebo komunikačního systému dodavatelem MUSÍ být definovány a dokumentovány následující požadavky:

- požadavky na licenční ujednání, vlastnictví kódu a práv duševního vlastnictví,

- požadavky na osvědčení kvality a správnosti provedených prací,
- požadavky na uložení zdrojového kódu,
- požadavky na právo přístupu k vývoji pro audit bezpečnosti a správnosti provedené práce,
- požadavky na smluvní podmínky na bezpečnost a zabezpečení kódu,
- požadavky na provedení testů zranitelností před instalací v produkčním prostředí.

1.1.15 Pro informační nebo komunikační systém vyvíjený externím dodavatelem MUSÍ být smluvně zajištěno právo auditu zdrojového kódu a dodržování požadavků na bezpečnost. Smluvně též MUSÍ být zajištěno uložení zdrojových kódů u důvěryhodné třetí strany (code escrow) v případě, že dodavatel nepředává zdrojový kód jako součást dodávky vyvíjeného programového vybavení (informačního nebo komunikačního systému systému).

1.1.16 V případě webových aplikací dodavatel MUSÍ zajistit vývoj dle principů definovaných ve standardu OWASP v aktuálním znění.

1.1.17 Správce informačního nebo komunikačního systému MUSÍ definovat a dokumentovat akceptační kritéria bezpečnosti pro přechod informačního nebo komunikačního systému do produkčního provozu.

2 Řízení zranitelností

MUSÍ být nastaveny adekvátní postupy pro řízení zranitelností.

Implementační pokyny:

2.1.1 Viz směrnice Řízení technických zranitelností.

3 Poskytování a nabývání licencí programového vybavení a informací

Společnost MUSÍ nastavit politiky pro poskytování a nabývání licencí programového vybavení a informací.

3.1 Pravidla a postupy nasazení programového vybavení a informací

3.1.1 K zajištění oprávněnosti používat nakupovaný počítačový program pověřený útvar MUSÍ:

- počítačový program, pokud nebyl vytvořen v rámci společnosti, pořizovat akvizicí pouze u výrobců, jejich autorizovaných dealerů či distributorů počítačových programů, kteří mají právo daný počítačový program distribuovat konečným uživatelům, a za tímto účelem požadovat od dodavatelů počítačových programů příslušná ujištění v rámci smluv na dodávky počítačových programů,
- v případě, že je počítačový program již nainstalován na nakupovaném hardwaru, požadovat od dodavatelů hardwaru písemná ujištění o tom, že jsou oprávněni počítačové programy instalovat, že instalací počítačového programu nebyla porušena práva k softwaru.
- programové balíky pořizovat pouze v originálních baleních a na originálních záznamových mediích, s výjimkou počítačových programů instalovaných pomocí dálkového přístupu,
- k počítačovým programům požadovat originální instalační média a uživatelskou dokumentaci, s výjimkou počítačových programů instalovaných pomocí dálkového přístupu,

- zajistit řádné převzetí a uložení originální smluvní, licenční a jiné dokumentace v rozsahu umožňujícím prokázat oprávněnost používaní počítačového programu (např. standardních licenčních podmínek, standardních podmínek pro údržbu a podporu, dodací listy, faktury),
- dodržovat zákon č. 148/1998 Sb. o ochraně utajovaných skutečností a zákona č. 110/2019 Sb. o zpracování osobních údajů,
- zajistit řádné registrování užívání počítačových programů v registračních centrech či obdobných evidencích výrobců počítačových programů v případě, že je registrace licenční smlouvou požadována. Registraci lze provést i elektronicky.

3.2 Evidence licencí

3.2.1 V případě, že nejde o volně šiřitelné počítačové programy, je základním dokladem o jeho oprávněném použití zaplacená faktura. Oprávněnost používání počítačových programů MŮŽE být dále prokázána zejména některými z následujících dokumentů:

- smlouvami na dodávky počítačového programu (pokud byly takovéto smlouvy uzavřeny),
- nabývacími doklady,
- licenčními smlouvami upravujícími užívání počítačového programu případně originálními standardizovanými licenčními podmínkami,
- doklady týkajícími se registrace užívání v registračním centru nebo obdobné evidenci výrobce či distributora počítačových programů (např. kopie registračních karet),
- elektronickými kopiemi odeslaných a přijatých zpráv v případě pořízení počítačových programů dálkovým přístupem.

3.2.2 Výše zmíněné dokumenty MUSÍ být evidovány o veškerých užívaných počítačových programech na jediném místě.

3.2.3 Odpovědnost za řádné vedení a evidenci nabývací dokumentace nesou příslušné útvary společnosti. Zároveň jsou tyto útvary MUSÍ zajistit u počítačových programů nově pořizovaných po nabytí účinnosti těchto pravidel uložení a evidenci originálních instalačních médií po celou dobu užívání počítačového programu.

3.2.4 Kromě dokumentace, týkající se samotného nabytí počítačových programů, MUSÍ být zajištěno centrální vedení evidence o instalaci počítačového programu. Účelem takovéto evidence je doložení způsobu, jakým došlo k instalaci počítačového programu, zejména ve vztahu k počtu počítačů, na kterých byl počítačový program nainstalován. Vedení evidence může být v elektronické podobě, v případě že bude zaručena autorizace záznamu.

3.2.5 Ke každému počítači užívaném v rámci společnosti MUSÍ být zajištěno vytvoření dokladu v písemné nebo elektronické formě (tzv. specifikační list), ve kterém jsou uvedeny všechny počítačové programy, oprávněně nainstalované a užívané na tomto počítači. Tento doklad musí být při každé změně nebo doplnění podepsán pověřeným zástupcem společnosti, dále fyzickou osobou, která provedla instalaci (pokud instalaci neprovedl pověřený zástupce společnosti) a oprávněným uživatelem (uživateli) příslušné stanice. Jsou-li užity typové konfigurace počítačového programu na více stanicích, lze vést specifikační list pro všechny tyto stanice společně jako jediný doklad. Vedení evidence může být v elektronické podobě, v případě že bude zaručena autorizace záznamu. Tento doklad musí být veden a musí být řádně doplňován ve všech případech změn konfigurace počítačových programů na počítači, tedy zejména v případech:

- odinstalování určitého počítačového programu,
- instalace nového počítačového programu,
- aktualizace stávajícího počítačového programu.

3.2.6 V případě, že daný počítačový program nemá nebo nemůže být dále používán vzhledem k morální opotřebovanosti, rozhodnutí o migraci funkcí, či přechodu na jiné softwarové prostředí nebo z jiného důvodu, provede se jeho vyřazení. O vyřazení počítačového programu MUSÍ být proveden zápis (protokol o vyřazení). Vyřazení probíhá v souladu s předpisy platnými pro likvidaci majetku u povinného subjektu.

3.2.7 Při převodu práv se MUSÍ postupovat v souladu s ustanoveními licenční smlouvy (např. oznámení dodavateli nebo na registrační místo).

3.3 Pravidla a postupy pro kontrolu dodržování licenčních podmínek

3.3.1 Společnost MUSÍ zajistit minimálně jednou ročně provádění pravidelných kontrol dodržování licenčních smluv platných pro nainstalované počítačové programy na všech počítačích a pracovních stanicích využívaných v rámci společnosti. O kontrolách a jejich výsledcích musí být vedeny záznamy, uchovávané u povinných subjektů po dobu nejméně tří let.

Použité zdroje

(1) ČESKÁ REPUBLIKA. Vyhláška 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. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

(2) *MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD* [online]. Verze 1.0. NÚKIB, 2020 [cit. 2022-04-20]. Dostupné z: https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf

(3) ČESKÁ REPUBLIKA. *USNESENÍ VLÁDY ČESKÉ REPUBLIKY č. 624/2001: Pravidla, zásady a způsob zabezpečování kontroly užívání počítačových programů*. In: . Praha, 2001. Dostupné také z: https://ezu.cz/app/uploads/2019/04/usneseni_vlady_624_2001.pdf

Příloha A: Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)