MINISTERSTVO ZEMĚDĚLSTVÍ, Těšnov 17, 110117 00 Praha 1

Standard systémové bezpečnosti

Označení: SSB
Verze: 2.0

Platnost od: 6. 1. 2017

Aktuální verze dokumentu je dostupná na: Intranetu MZe

	Údaje o vydání		
	Zpracoval:	**Odpovědný pracovník:**	**Schválil:**
Funkce:	Architekt kybernetické bezpečnosti	Manažer kybernetické bezpečnosti	Manažer kybernetické bezpečnosti
Jméno:	*Roman Smetana*	*Ing. Karel Štefl*	*Ing. Karel Štefl*

Obsah:

1. Úvodní ustanovení

1.1. Účel standardu

Účelem standardu je definovat základní rámec pro implementaci bezpečnosti aplikací a systémů zaváděných nebo provozovaných v infrastruktuře MZe.
Tento rámec je tvořen vymezením bezpečnostních požadavků, které musí splňovat aplikace a systémy vyvíjené, dodávané a rozvíjené v prostředí MZe. Jedná se o definované procesy, postupy, opatření a jejich naplnění vzhledem k požadované úrovni zabezpečení.
Cílem naplnění standardu systémové bezpečnosti je sjednotit požadavky na povýšení bezpečnosti u všech dodávaných, vyvíjených nebo rozvíjených systémů. Předmětem standardu jsou tedy rozvíjené nebo vyvíjené a dodávané aplikace, informační systémy na míru nebo podobné programy a řešení, a dále i komerční software, které jsou dodávány za účelem poskytování agendy a její podpory vymezené zákonem nebo poskytování informačních služeb pro interní potřeby v prostředí MZe (dále jen „Systém“).

1.2. Rozsah působnosti

Standard je závazný pro všechny zaměstnance MZe, a to jak ve služebním, popřípadě pracovním poměru, tak i zaměstnaných na základě dohod o pracích konaných mimo služební, popřípadě pracovní poměr (dále jen „zaměstnanci“), a dále pro všechny osoby a externí strany vykonávající práce pro MZe na základě smluvního vztahu či občanského zákoníku (dále jen „externisté“), kteří spolupůsobí při rozvoji, vývoji nebo zavádění Systému.

1.3. Pojmy a zkratky

Pojmy a zkratky používané v tomto standardu jsou uvedeny v tabulce na konci tohoto dokumentu.

2. Rozdělení a definice požadavků na zabezpečení

Požadavky na zabezpečení Systému jsou v tomto dokumentu rozděleny na čtyři základní oblasti, vztahující se k jednotlivým atributům bezpečnosti, tak jak jsou chápány obecně i směrem k bezpečnosti Systému. Jedná se o tyto oblasti:

2.1. Důvěrnost

Musí být zajištěna mechanismy se schopností ujistit se, že je vynucena nezbytná úroveň míry utajení v každém okamžiku, kdy dochází ke zpracování dat a je zajištěna prevence jejich neautorizovaného vyzrazení. Taková úroveň důvěrnosti musí přetrvat minimálně během uchovávání dat v Systému a při jejich přenosu k adresátovi.

2.2. Integrita

Musí být zajištěna identifikací přesnosti, zaručeného obsahu a musí být provedena opatření proti jejich neautorizované změně. Hardwarové, softwarové a komunikační prostředky musí pracovat tak, aby data uchovávaly a zpracovávaly správně a přesně, přenášely je do požadovaného cíle bez nežádoucích změn. Celkově musí být Systém a síť chráněny před vnějším rušením či kontaminací původní informace.

2.3. Dostupnost

Musí být zajištěna spolehlivou a včasnou dispozicí dat a zdrojů autorizovaným jednotlivcům. Systém a sítě musí mít datovou kapacitu dimenzovanou tak, aby v definovaném čase poskytovaly dostatečný výkon, a musí být schopny zotavit se z výpadků transparentním a rychlým způsobem. Proto musí být zavedeny redundantní mechanismy a navrženy záložní řešení pro možnost rychlé náhrady. Součástí proškolení uživatelů k Systému musí být postup nebo návod jak provést jeho uvedení do funkčního stavu.

2.4. Metodika vývoje a ostatní požadavky

Představuje zavedení souhrnu postupů, pravidel a nástrojů používaných pro návrh, plánování a řízení vývoje software. Metodikou se též rozumí využití těchto položek nebo dalších specifických postupů pracovním týmem nebo celou organizací při vývoji aplikačního software nebo informačního.

3. Požadavky na Systém

3.1. DŮVĚRNOST

3.1.1. Řízení přístupu

Systém musí zajišťovat tvz. AAA (Autentizaci, Autorizaci, Audit) v potřebné úrovni dle jeho konkrétní specifikace.

- Systémy, které obsahují citlivá data, musí podporovat vícefaktorovou autentizaci.
- Systémy typu webové aplikace musí umožňovat autentizaci zašifrovaným kanálem (pomocí TLS), tak, aby přihlašovací údaje neprocházely síťovou infrastrukturou v otevřeném tvaru.Musí existovat možnost oddělení rolí v Systému, minimálně pro:
    - administrátory,
    - uživatele,
    - auditory.
- Správa interních a externích uživatelských entit musí být oddělena.
- Musí existovat možnost šifrování přenosu i uložení citlivých uživatelských dat.

Registrace, autentizace a identifikace uživatelů.

Systém musí umožňovat:

- registraci všech uživatelů centrálně,
- stanovit pravidla pro procesy:
    - registrace,
    - schvalování,
    - generování identit,
    - přidělování a odebírání přístupů,
    - deaktivace identit,
    - monitorování činnosti uživatelů.

Tyto funkce musí být v Systému buď přímo implementovány, nebo může Systém využívat stávajících podsystémů pro podporu identifikace a autentizace v prostředí MZe.

Pokud v rámci Systému nebo jeho komponent a podpůrných podsystémů existují lokální účty, musí se řídit následující politikou hesel pro privilegované účty nebo musí umožnit integraci se systémem pro správu privilegovaných účtů.

Politika hesel pro privilegované účty:

- minimální účinná délka hesla je 17 znaků;
- při tvorbě hesla se musí povinně použít:
  - alespoň dvě malá písmena (a-z),
  - alespoň dvě velká písmena (A-Z),
  - alespoň dvě číslice (0–9),
  - alespoň dva speciální znaky (např. / * . - +),
- platnost hesla 90 dní,
- zákaz používaní stejného hesla (posledních 24 hesel),
- minimální platnost hesla 24 hodin,
- zamčení účtu po množství pokusů: 5,
- jednorázové prvotní heslo.

Řízení hesel je vázáno na aktuální bezpečnostní politiku platnou v době implementace řešení a v závislosti na její definici se parametry politiky pro vytváření hesel mohou měnit. Dodavatel Systému se při tom musí řídit aktuálním zněním směrnice.

3.1.2. Autorizace

Autorizace uživatelů musí probíhat na základě stanovených uživatelských rolí. Pro ověření uživatelů v Systému musí být přímo v něm implementována funkce ověření uživatelů nebo musí využívat stávajících systémů pro podporu autorizace v prostředí MZe. Současné ověřování uživatelů je řízeno adresářovou službou (LDAP) resp. jejich členstvím ve skupinách (tedy LDAP skupina = role v Systému). Systém musí mít vyhrazenu větev LDAP adresáře, ve kterém existují vlastní skupiny. Systém se pomocí protokolu LDAP připojí do LDAP adresáře, ze kterého následně vyčítá informace o členství ve skupinách, na základě kterých se dále rozhoduje o autorizaci (oprávnění). Pokud bude nutné z důvodu komplexnosti a složité údržby (např. oprávnění přístupu k jednotlivým objektům) udržovat některá oprávnění pouze lokálně, musí být udělena výjimka manažerem kybernetické bezpečnosti. Systém musí navíc v takovém případě poskytovat vhodné rozhraní pro jejich export, včetně vazeb na uživatele (webová služba, JDBC, soubor).
Pro Systém musí být definovány samostatné uživatelské role, které se dále člení dle aplikačních požadavků.

3.1.3. Infrastrukturní privilegované účty

Na všech podpůrných systémech a komponentách (OS, DB, atp.) musí být zavedeny privilegované účty, výhradně personifikované, které představují přidělení samostatných přihlašovacích údajů pro jednotlivé administrátory. Použití sdílených administrátorských účtů musí být řádně odůvodněno a schváleno výjimkou manažera kybernetické bezpečnosti MZe.

3.1.4. Servisní účty

Servisní nebo také technické účty, pod kterými běží Systém či jeho jednotlivé komponenty, pod kterými jsou jakýmkoli způsobem impersonifikována vlákna, systémová či meziprocesová volání, nebo prostřednictvím kterých Systém přistupuje k ostatním komponentám nebo externím systémům, musí být uvedeny v dokumentaci k Systému. U každého účtu musí být uveden jeho účel a způsob jakým je možné účtu změnit heslo, včetně identifikace všech míst, kde je takové heslo uloženo (DB tabulka, konfigurační soubor, atp.).

Hesla k servisním účtům musí být předána MZe bezpečným způsobem dle smluvně stanovených podmínek.

3.1.5. Omezení oprávnění

Pro všechny typy účtů (uživatelské, administrátorské, servisní) je vždy uplatněn “princip minimálních oprávnění“ (princliple of least privilege), tedy že každý účet má nastavena pouze taková oprávnění, která jsou nezbytná pro provádění činností, ke kterým byl účet zřízen. Princip minimálních oprávnění se vztahuje též na oprávnění ke stránkám v režimu chráněné paměti.
Pro servisní účty se dále uplatňuje “princip oddělení privilegií“ (principle of privilege separation), na základě kterého má každá komponenta (funkční část) pouze taková oprávnění, která potřebuje pro svoji funkci a tedy využívá svůj vyhrazený servisní účet s příslušnými oprávněními.

3.1.6. Procesní řízení účtů

Proces **přidělování/odebíraní oprávnění** a **vytváření/rušení účtů** v Systému a podpůrných komponentách (OS, DB, atp.) je řízen současně platnou směrnicí MZe (BIT 08), tedy vždy je nutné podat formální žádost, která musí projít zavedeným schvalovacím workflow. V případě existence lokálních oprávnění, která jsou řízena jiným způsobem, musí být jasně popsán proces jejich přidělování/odebíraní, který musí být odsouhlasen manažerem kybernetické bezpečnosti MZe.

3.1.7. Auditní mechanismy Systému.

S ohledem na požadavek zajištění auditovatelnosti dat i procesů v Systému je nezbytně nutné zabudovat tuto možnost při návrhu a vývoji Systému. Jedná se zejména o přístupy i změny v datech pro jednotlivé objekty. Rovněž proces řízení identit uživatelů musí být auditovatelný.

Logy Systému musí být integrovány do aktuálního centrálního řešení pro správu a vyhodnocování logů (v současnosti SIEM - HP ArcSight), které je provozováno v prostředí MZe. Systém tedy musí umožnit takovou integraci. Logy Systému musejí být dostupné bez prodlení od vzniku události, a integrovány do SIEM v jím podporovaných formátech minimálně jednou z následujících metod:

- Syslog
- SNMP TRAP
- Textový soubor
- JDBC
- Microsoft Event Log

Systém, včetně infrastruktury, která je jeho podpůrnou součástí, a jeho další komponenty, musí být připraveny na integraci do SIEM obdobným způsobem tak, aby naplňovaly požadavky na bezpečnostní monitoring definované dále.

Dodavatel Systému zajistí definici rozsahu Systému vzhledem k infrastruktuře a tedy, které části infrastruktury a podpůrné komponenty jsou jeho součástí a doporučí vzhledem k bezpečnostním dopadům jejich bezpečnostní monitoring. Detailní specifikace nastavení

Systémů pro integraci se SIEM se řídí standardy MZe, (standardy SIEM pro jednotlivé Systémy). Dodavatel zajistí přístup k auditním logům a doporučí způsob jejich vyčítání v souladu s těmito standardy.

V rámci MZe musí být pořizovány a uchovávány auditní záznamy zejména takové, které jsou uvedeny ve výčtu níže, tak, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování bezpečnostních incidentů. Zaznamenávání událostí zohledňuje technické možnosti Systému a pro sběr záznamů ukládá minimálně tyto typy událostí:

- přihlášení a odhlášení uživatelů a administrátorů,
- činnosti provedené administrátory,
    - použití privilegovaných účtů, např. účtu supervisora, administrátora,
    - spuštění a ukončení Systému,
    - změny konfigurací,
- činnosti vedoucí ke změně přístupových oprávnění,
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- zahájení a ukončení činností technických aktiv,
- automatická varovná nebo chybová hlášení technických aktiv,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Jednotlivé položky logu Systému nebo jeho jednotlivé řádky záznamu musí obsahovat minimálně tyto pole:

- ID záznamu
- Datum a čas události (uvedený s jednoznačnou identifikací časové zóny, např UTC nebo lokální čas s uvedením offsetu)
- síťové identifikátory komunikujících bodů (tj. např. IP adresy a porty)
- Uživatelský identifikátor
- ID Typu události
- Popis události
- Detail události

Textová pole musí být oddělena pomocí znaku„|“ (pipe, ASCII kód 124) a musí být vytvořen číselník ID typu událostí dle typických událostí v Systému a předán v dokumentaci.

Pokud údaje zapisované do logu Systému obsahují citlivá data (heslo, klíč či jeho prekurzor, session ID apod.) nesmí být uložena v plain textu, ale musí být před zapsáním zašifrovány nebo přepsány pseudonáhodnou sekvencí;

V Systému musí být zavedena ochrana proti deaktivaci, selhání či změnám v pořizování auditních záznamů a ochrana proti změnám nebo zničení auditních záznamů.
Přístup k auditním záznamům musí být bezpečně chráněn, aby bylo zabráněno jeho zneužití nebo ohrožení. Systém musí umožnit nastavení přístupových práv k auditním záznamům tak, aby mohly být auditovány samostatnou rolí (auditor, security officer a.p.).

3.1.8. Šifrování

Veškerá citlivá data musí být adekvátním způsobem zabezpečena kryptografickými metodami, které zajistí pouze autorizovaný přístup. Ochrana dat musí být zaručena během

celého jejich životního cyklu, tedy jak při jejich přenosu tak jejich uchovávání. V rámci kryptografických metod musí být Systém připraven na využívání kryptografických algoritmů, které jsou v souladu s Přílohou č. 3 k vyhlášce č. 316/2014 Sb., (vyhláška o kybernetické bezpečnosti).

Závazné detaily nastavení šifrování k jednotlivým protokolům jsou definovány ve zde vloženém dokumentu, a to vždy v jeho aktuální verzi:

požadavky OKB MZe na kryptografii

3.1.9. Certifikační autority a PKI.

Systém musí být připraven využívat při autentizaci uživatele a ověřování digitálního podpisu kvalifikované certifikační autority v ČR a ze zemí EU, interní CA MZe, případně jinou CA nastavenou jako důvěryhodnou.

Systém musí umožnit elektronické podepisování a schvalování dokumentů prostřednictvím zapojení do procesů interního PKI pro správu uživatelských klíčů nebo pro vytváření elektronických značek a pro autoritu časových razítek, pokud Systém tyto procesy využívá. Ve všech těchto případech se Systém též musí řídit certifikační politikou a prováděcími směrnicemi zúčastněných CA.

Při ověřování certifikátu, ať už jde o certifikát protistrany v komunikaci nebo certifikát pro ověření elektronického podpisu či časového razítka, musí Systém implementovat algoritmus ověření certifikátu minimálně s těmito kontrolami:

- sestavení certifikační cesty až k důvěryhodnému certifikátu
  - lze použít atribut AIA k dotažení certifikátů mezilehlých CA
  - musí být možnost použít statickou cache certifikátů mezilehlých CA
  - preferovaně používat certifikáty mezilehlých CA, které jsou součástí TLS handshake či obálky elektronického podpisu
  - neúspěšné sestavení jedné certifikační cesty není samo o sobě důvodem pro ukončení ověřování certifikátu s negativním výsledkem, pokud lze sestavit alternativní certifikační cesty (např. v prostředí s křížovou certifikací kořenových CA)
- pro všechny certifikáty v certifikační cestě, které nejsou explicitně důvěryhodné, je nutno ověřit:
  - uvedení daného certifikátu podle jeho hashe či hashe veřejné části jeho klíče na seznamu explicitně nedůvěryhodných certifikátů
  - platnost certifikátu vzhledem k
    - aktuálnímu času
    - nebo k času podpisu, pokud je tato hodnota v ověřitelné časové značce svázané s ověřovanými daty (kontrasignace TSA)
  - atributy Basic Constraints (Entity Type, Path Length Constraint), Name Constraints, Key Usage a Extended Key Usage, jsou-li v certifikátu uvedené, pro dané použití certifikátu a klíče, a to bez ohledu na jejich kritičnost
  - sílu podpisového algoritmu, popř. i ve vztahu k době platnosti a/nebo aktuálnímu času, pokud je použití daného algoritmu či velikosti klíče časově omezeno

- platnost digitálního podpisu veřejnou částí klíče nadřízené CA
- OID certifikační politiky, pokud je pro dané použití omezena
- zneplatnění certifikátu před koncem doby platnosti podle:
  - CRL
    - lze použít atribut CRL DP pro dotažení aktuálního CRL
    - musí být možnost použít statickou cache s CRL
  - OCSP
    - online komunikací s OCSP responderem podle URL v atributu AIA
    - OSCP stapling, pokud jej daný protokol (např. TLS) podporuje
- v případě, že certifikát obsahuje atribut (atributy), označený (označené) jako kritické, které ověřovací algoritmus buď nezná, nebo nemůže jejich kontrolu z nějakého důvodu provést (např. kvůli chybě v komunikaci), musí být ověřování certifikátu ukončeno jako neúspěšné
- pokud ověřování v certifikační cestě není úspěšné
  - je možné použít alternativní certifikační cesty, pokud je lze sestavit (např. v prostředí s křížovou certifikací kořenových CA)
  - v případě, že se selhání váže k obsahu či stavu platnosti koncového certifikátu, alternativní cesty se již nepoužijí

- pokud se ověření certifikátu váže na identitu protistrany (hostname v URL, IP adresa vzdáleného konce IPSec apod.) či původce (např. E-mailová adresa odesilatele podepsané zprávy), pak pro porovnání:
  - pokud není přítomen atribut Subject Alternative Name (SAN), použije se atribut Subject
  - pokud je přítomen atribut SAN, použije se preferovaně ten; volitelně, pokud se nenalezne shoda v atributu SAN, může se použít i atribut Subject

3.2. INTEGRITA

Cílem je zaručení a udržení konzistence a správnosti dat během jejich celého životního cyklu. Je tedy potřeba zajistit, aby data nemohla být neautorizovaně modifikována a aby každá autorizovaná i neautorizována modifikace dat byla detekována a zaznamenána. Spolu s integritou je žádoucí zajistit také nepopiratelnost, tedy vyloučení možnosti popřít provedení libovolné operace nad daty. V základu je integrita dat zajištěna pomocí vhodného řízení přístupu k datům (autorizace) a auditovatelnosti (logování a následná detekce přístupu k datům). Integrita kritických dat musí být zajištěna implementací dodatečných kontrol – např. počítání kontrolních otisků dat a jejich pravidelná kontrola, dále též kryptografické zajištění kontrolních otisků dat (elektronický podpis, HMAC, hash tree).
Každý vstup do Systému (externí systém, uživatel, mezi komponentami) je vždy kontrolován na typovou a logickou správnost, čímž může být detekováno poškození dat, nebo případný pokus o útok. V definovaných případech se provádí validace dat dle specifikace v zadávací dokumentaci, ta určuje základní parametry a určuje kvalitu vstupů se zaměřením např. na kontrolu správného formátu dat, kontrolu mezí, přítomnost povinných dat, logických závislostí mezi daty apod. Architektura řešení bere v úvahu bezpečnostní aspekty prostředí. Systém musí být navržen mimo jiné tak, aby respektoval jednotlivé bezpečnostní přiřazení komponent Systému k zónám důvěryhodnosti a jejich rozmístění do jednotlivých bezpečnostních zón prostředí.

3.3. DOSTUPNOST

Dostupnost Systému musí být stanovena a definována na požadovanou úroveň. Podle této definice se dále stanoví architektura celého řešení s ohledem na dostupnost, ve smyslu redundantních a clusterovaných schémat v režimu vysoké dostupnosti (HA), stanovení úrovně podpory, DRP a zálohování.

3.3.1. Řešení vysoké dostupnosti (HA)

Dodavatel Systému navrhne v rámci architektury řešení, způsob zajištění vysoké dostupnosti Systému dle jeho definice úrovně dostupnosti. Ta musí být zajištěna pomocí redundantních nebo clusterovaných schémat přímo v návrhu architektury.

Postupy obnovy po havárii - Disaster recovery planning

Dodavatel Systému navrhne postupy pro vypnutí a zapnutí Systému, včetně posloupnosti jednotlivých kroků, především s ohledem na bezpečné obnovení Systému při jeho selhání – tj. vytvoření plánů obnovy aplikace. Dále je povinen spolupracovat na jeho ověření v rámci testování obecných plánů obnovy provozu Systému MZE, uvedené též v části Testování.

3.3.2. SPOF

Při návrhu HW platformy, logické a fyzické komunikace a datových toků obecně, musí být zohledněno dodržování pravidla eliminace „SPOF“ (Single Point of Failure) – tedy, že porucha jedné komponenty nezpůsobí výpadek celého Systému. Jedná se o serverovou infrastrukturu, datové úložiště, zálohování a další prvky celé LAN.

3.3.3. Zálohování

Návrh Systému musí obsahovat požadavky na zálohování, které vychází ze SLA parametrů aplikace. Vždy se požaduje vytvoření detailního návrhu zálohování celého Systému včetně návaznosti na stávající zálohovací systém MZe. Popis by měl mít strukturu, viz vzor níže

Server	Co zálohovat	Jak často full backup	Kolik záloh držet	Kolik dní držet zálohy	Jak často inkrement backup	Kdy probíhá záloha	Předpokládaná doba obnovy
Server-x	Celý server	1*týdně	30		denně	18:00-18:10	30 minut
Server-x	Databáze A	2*denně	28			8:00-8:10, 20:00-20:10	10 minut
Server-x	Databáze A – transakční logy			730	Každou transakci	Dle transakcí	10 minut
Aktivní prvek-X	Konfigurační soubory	Při každé změně	10			Dle změn	30 minut

3.4. METODOLOGIE PRO VÝVOJ A OSTATNÍ POŽADAVKY

Dodavatel musí mít formalizovanou Metodologii pro vývoj, programování a kódování aplikace zahrnující i požadavky na bezpečnost, včetně opatření na ochranu proti škodlivým programům nebo postupům. Metodologie musí též zahrnovat základní principy organizační bezpečnosti pro vývoj a testování aplikace. Dodavatelé musí doložit typ metodologie, který použil pro vývoj aplikace prostřednictvím čestného prohlášení a dodání popisu nebo dokumentace této metodologie.

3.4.1. Data

Systém musí poskytovat podporu pro správu klasifikovaných dat.

Dále pak je požadováno, aby řešil vstupně - výstupní validaci dat tak, aby odesílaná a přijímaná data byla kontrolována na typovou a logickou správnost při jejich zadávání nebo exportu.
Šifrování ukládaných dat musí být prováděno s ohledem na požadavky zajištění důvěrnosti dat, kde je vždy nutné využít vhodného šifrování ukládaných dat, které zajistí tento požadavek na důvěrnost viz kapitola 3.1.9.

3.4.2. Lokalizace

Systém musí podporovat českou národní lokalizaci a přednostně vícebajtové kódování (UTF8 s povinností uvádět BOM).

3.4.3. Výjimky běhu, chyby a hlášení

Systém musí podporovat řízení výjimek, kdy výjimkou se myslí libovolná chyba nebo neočekávané chování, které se vyskytne během vykonávání programu a je následně zpracováno a zároveň nedojde k neřízenému selhání běhu.

3.4.4. Práce s pamětí

Kód Systému musí implementovat vhodná opatření při práci s pamětí:

- již nepoužívané objekty a jiné datové struktury jsou z paměti odstraňovány;
- pokud datová struktura obsahuje citlivá data (heslo, klíč či jeho prekurzor, session ID apod.), musí být před dealokací tyto hodnoty přepsány pseudonáhodnou sekvencí;
- je nutné zajistit, aby datovou strukturu, označenou k dealokaci, nebylo možné dereferencovat (tj. odstranit před dealokací všechny ukazatele na dealokovanou strukturu);
- paměťové stránky, které obsahují pouze data, nebyly zároveň označeny jako stránky se spustitelným kódem;
- nepřímé skoky (např. volání virtuální metody) musí před vlastním provedením volání zkontrolovat, zdali je adresa volaného kódu legitimní.

3.4.5. Řízení konfigurace a změn

Systém musí mít zavedeno řízení konfigurace a změn, které představuje systematické vyhodnocování, koordinování a implementaci schválených změn, včetně uchování předchozích verzí a testování verzí nových.

3.4.6. Bezpečnost, provoz a správa Systému v prostředí MZe

Při implementaci Systému je nutné vždy zhodnotit dopady požadavků na provoz. Při začlenění do infrastruktury MZe je nezbytné brát v úvahu důsledné oddělení interní sítě a zabezpečení firewally. Z tohoto důvodu je nutné, aby při návrhu realizace byly stanoveny potřebné požadavky na úpravy provozní a bezpečnostní infrastruktury. Provoz aplikace respektuje architekturu řešení, především vyžadovanou lokalizaci jednotlivých funkčních komponent v odpovídajících bezpečnostních zónách, např. Systém poskytující data do internetu musí být umístěn v samostatně odděleném segmentu sítě (DMZ) apod. a to dle členění jednotlivých bezpečnostních zón a zón důvěryhodnosti (trust zones) v MZe

3.4.7. Ochrana Systému typu webové aplikace.

Části Systému typu webová aplikace musí být chráněny proti nejčastějším útokům, které byly identifikovány nezávislým společenstvím OWASP (http:www.owasp.org) tím, že se při vývoji použijí principy definované dle této metodiky v aktuálním znění. Podle dobré vžité praxe musí být pozornost věnována především následujícím známým zranitelnostem:

- Cross Site Scripting (XSS). XSS je metoda narušení WWW stránek využitím bezpečnostních chyb ve skriptech (především neošetřené vstupy).
- Injection útoky. SQL injection je technika napadnutí databázové vrstvy programu vsunutím (injection) kódu přes neošetřený vstup a vykonání vlastního, pozměněného, SQL dotazu. Vedle SQL injection existují též další podobné scénáře s jiným cílem, např. shell command injection, LDAP injection atd.
- UmístěníVzdálené spuštění kódu a to buď vlivem zranitelnosti v samotném webovém serveru, použitém frameworku či logice ve webové aplikaci.
- Nezabezpečený přímý popis objektu. Zranitelnosti této kategorie umožňují útočníkovi získat informace o jednotlivých objektech cílové aplikace bez patřičné autentizace.
- Cross Site Request Forgery (CSRF). CSFR je technika, která umožňuje útočníkovi podvrhnout formulář na jiné stránce nebo pomocí některých HTTP metod přesměrovat prohlížeč oběti na skript zpracovávající legitimní formulář aplikace s daty, která můžou oběť poškodit.
- Únik informací nebo nedostatečné řízení chyb. Zranitelnosti tohoto typu útočníkovi zpřístupňují v případě chybového stavu aplikace informace, které lze později použít k lepšímu plánování útoku.
- Špatná autentizace a správa relace. Zranitelnosti tohoto typu umožňují útok na přihlašovací části aplikace či úplné obcházení přihlašovacího systému.
- Nezabezpečené kryptografické úložiště. Zranitelnosti tohoto typu můžou způsobit kompromitaci privátního šifrovacího klíče jedné či obou stran spojení.
- Nezabezpečená komunikace. Zranitelnosti tohoto typu umožňují útočníkům odchytávat komunikaci, která jim není určená, a provádět též aktivní útoky typu Man-in-the-Middle.
- Chybné zamezení URL přístupu. V případě, že aplikace umožňuje neautentizovaný přístup i ke stránkám, ke kterým by měl být přístup jen po příslušné autentizaci, je možnou zranitelností situace, kdy takto odkazovaná stránka zobrazí některé informace, které by měly být přístupné jen konkrétním autorizovaným uživatelům, či systémové informace citlivého charakteru.

Zjištění některé z výše uvedených bezpečnostních zranitelností, případně jiných zranitelností známých v okamžiku vývoje webové aplikace je považováno za vadu vytvořené aplikace.

Při použití XML komunikace by měly být prováděné tyto kontroly:

- Početní a délkové limity
  - Maximální počet atributů v elementu
  - Maximální počet namespaces, namespace prefixů a obecně všech lokálních jmen v XML dokumentu
  - Maximální délka jména elementu
  - Maximální délka jména atributu
  - Maximální délka identifikátoru namespace (URI)
- Znakové sady
  - Konzistence deklarací (atribut „charset“ v HTTP request hlavičce „Content-Type“, BOM na začátku dat a atribut „encoding“ v hlavičce XML)
  - Přítomnost netisknutelných znaků
- Escaping
  - Escaping validních znaků (např. „A“ místo „A“, též např. „Я“ místo „Я“, pokud je použitý encoding některý z UTF apod.)
  - Použití znaku „&“ mimo escape sekvenci
  - Použití znaků „“ (uvozovky – ASCII 34), „’“ (apostrof – 39), „<“ a „>“ mimo místa, kde mají syntaktický význam
  - Kontrola správného ohraničení CDATA sekcí (pokud se vůbec mohou vyskytovat, pokud ne, tak rovnou odmítat XML zprávy, které CDATA obsahují)
- Přítomnost XML External Entity v DTD

Při použití JSON formátu pro výměnu dat by měly být prováděné minimálně tyto kontroly:

- maximální velikost zprávy
- maximální délka názvu klíče
- neunikátní klíče
- maximální počet elementů
- maximální úroveň vnoření
- maximální velikost pole (myšleno array, nikoli field)
- komentáře, pokud jsou zakázané nebo limitované velikostí
- limit objemu whitespace (tabulátory, mezery, odřádkování)
- kontrola striktní syntaxe a struktury JSON dokumentu (některé parsery v aplikacích ledacos tolerují)
- kontrola kanonické formy nebo provedení kanonizace (pokud je požadována)
- kontrola obsahu (jména klíčů, hodnoty) na sekvence XSS či SQLi (s možností vypnout per element – nemusí být datově transparentní a někdy může hodnota naopak záměrně obsahovat renderované HTML)
- provádí se kontrola syntaxe kódu JSON – parser pro RFC4627
- validace key value, metoda zjišťuje, zda hodnoty použité v key value odpovídají typu definované hodnoty (numeric,boolean apod.)

3.4.8. Antivirová ochrana

Pro implementaci Systému musí být navržen způsob antivirové ochrany především pomocí stávajících řešení používaných v prostředí MZe. Dodavadavtel zhodnotí všechny směry a vstupy dat do Systému a navrhne způsob antivirové kontroly. Vezme přitom v úvahu existující antivirové nástroje MZe a jejich standardy.

3.4.9. Testování Systému.

Testování Systému musí probíhat v souladu s metodologií vývoje.

Integrační testy, systémové, zátěžové a akceptační testy musí vždy probíhat ve vyhrazeném testovacím prostředí nebo módu, tak aby nemohla být narušena činnost produkčních systémů. Penetrační a bezpečnostní testy probíhají i na produkčním prostředí a provádí je nezávislý auditor, tak aby byl zajištěn atribut nestrannosti. Scénáře penetračních a bezpečnostních testů musí být předem odsouhlaseny manažerem kybernetické bezpečnosti za stranu MZe. Penetrační nebo bezpečnostní testování včetně konfiguračního review, musí být provedeno po implementaci Systému a musí ověřit správnost nastavení celého prostředí.

Testovací údaje (data) musí být dostatečně chráněna a kontrolována. Je-li to možné, musí být testování prováděno na neprovozních datech. Pokud je nezbytné využít k testování provozní data, upřednostní se použití již neplatných dat. Při výběru provozních dat k testování z provozních databází je nutné použít maskování položek, které nejsou pro potřeby testování nezbytné.
Pokud je nutné použít platná provozní data, musí být dodrženy následující zásady:

- postupy kontroly přístupu platné pro provozní data musí být uplatněny i pro testovací data,
- každé kopírování provozních dat do testovacího prostředí musí být autorizováno souhlasem garanta IS a schválením pracovním týmem (například ve schváleném zápisu z pracovního týmu nebo HTP),
- neveřejné informace musí být okamžitě po ukončení testů odstraněny z testovaného prostředí bezpečným způsobem, aby nebyla možná jejich dodatečná obnova,

kopírování a užití provozních dat musí být zaznamenáváno do auditních záznamů.

Vyvíjené aplikace musí být prověřeny nástrojem pro analýzu zdrojového kódu a nástrojem na zjišťování zranitelností. Součástí akceptace musí být prohlášení o provedení těchto testů a jejich výsledky. Dodavatel Systému poskytne prohlášení o provedení těchto testů, které bude obsahovat minimálně tyto položky:

- Datum provedení testu
- Použitá testovací metodika a metodika scoringu
- Název nástroje použitého pro testování
- Konfigurace profilu pro testování
- Testovací protokol
- Výsledky testování, navržení protiopatření
- Shrnutí výsledku testování a závěrečná zpráva
- Osobní odpovědnost – jména odpovědných osob

3.4.10. Patch management

Testování musí probíhat i v dodavatelské i provozní fázi a to nejméně 1x za dva měsíce nebo v souvislosti s aktualizacemi Systému nebo dodání nových komponent při změnových řízeních apod. Dodavatel Systému navrhne v rámci patch managementu testování Systému a jeho běhu na OS s nově vydávanými bezpečnostními záplatami. V dodavatelské fázi je možné s ohledem na implementaci Systému udělit výjimku z patch managementu. Výjimku uděluje Manažer bezpečnosti.

3.4.11. Komunikace

Způsob řešení integrace na externí systémy.
Pokud Systém využívá data nebo služby externích systémů, musí být jejich integrace provedena prostřednictvím centrální komunikační sběrnice MZe. Podmínky a způsob jejího napojení jsou součástí metodiky závazných pravidel centrální komunikační sběrnice a dodavatel Systému musí požadavky tohoto dokumentu při integraci dodržovat.

Komunikace s externími systémy musí být rozdělena podle stupně zabezpečení na:

- Zabezpečený kanál přenosu (šifrování dat) s povinnou úrovní zabezpečení koncových bodů Systému na úrovni infrastruktury.
- Šifrování dat pro přenos a autorizací uživatele v rámci Systému.
- Zajištění šifrování nebo náhradu citlivých dat na úrovni poskytovatelských a konzumentských systémů pomocí end to end metody při přenosu dat pomocí centrální komunikační sběrnice. Např. pole nesoucí osobní data je nahrazeno identifikátorem nebo pomocí hash.

3.4.12. Fyzická bezpečnost a požadavky na infrastrukturu datových center.

Požadavky na fyzickou bezpečnost, nároky na HW platformu a infrastrukturu datových center jsou definovány v aktuální Směrnici k fyzické bezpečnosti a bezpečnosti prostředí MZe. Dodavatel Systému je povinen se jimi řídit a to do úrovně rozsahu Systému vzhledem k fyzické vrstvě.

Požadavky na HW platformu.
HW platforma - tj. hardwarová platforma i systémový software musí zajišťovat řádný a efektivní provoz Systému.

Požadavky na Infrastrukturu datových center.

Infrastruktura, musí splňovat požadavky zejména na:
• Zajištění ochrany prostor – bezpečnostní perimetr,
• Zabezpečení přístupu osob,
• Nezávislý zdroj elektrického proudu /UPS/,
• Přesná klimatizace prostor,
• Datové rozvody dle technických norem,
• Bezpečnost kabelových rozvodů,
• Zabezpečení a ochranu datové centra vč. elektronické zabezpečovací signalizace,
• Vícenásobné kapacitní připojení k internetu,
• Možnost vybudování vlastní optické konektivity.

3.4.13. Dokumentace

Dodávaná dokumentace Systému obsahuje položku bezpečnostní dokumentace.
Ta musí obsahovat popis všech relevantních bezpečnostních atributů pro dodávku Systému.

Kromě těchto atributů je vyžadováno schéma začlenění Systému a komunikační mapa na úrovni L2-L3 topologie. Dodavatel si vyžádá podkladové materiály, tak aby byl schopen vytvořit tuto komunikační mapu a schéma, a to již jako součást návrhu Systému.

4. Závěrečná ustanovení

- Za dodržování tohoto standardu odpovídají jednotliví představení příslušných organizačních útvarů MZe v rámci vymezených kompetencí.
- Za správnost a aktualizaci tohoto standardu odpovídá manažer kybernetické bezpečnosti.
- V případě, že jsou činnosti uvedené v tomto standardu upraveny zvláštním právním předpisem, postupuje se podle tohoto předpisu.
- Dnem účinnosti tohoto standardu se ruší veškeré předcházející verze tohoto standardu.
- Revize tohoto standardu se provádí v případě potřeby, minimálně však jednou za dva roky.
- Revize tohoto standardu se provádí též v případech opakovaného zjištění incidentů bezpečnosti informací, v případě významných změn v informačním systému a zpracovávaných informacích či v souvislosti s provedením revize BPI MZe.
- Za přípravu revizí tohoto standardu zodpovídá manažer kybernetické bezpečnosti.

Tabulka 1 - seznam zkratek

Termín	Význam
Internisté	Zaměstnanci a to jak v pracovním poměru, tak i zaměstnaných na základě dohod o pracích konaných mimo pracovní poměr
Externisté	Všechny osoby a externí strany vykonávající práce pro MZe na základě smluvního vztahu
Helpdesk	Specializované *oddělení Objednatele* zajišťující komplexně uživatelskou podporu
ITSM	IT service management – řízení úrovně poskytovaných Služeb především, nikoliv však výhradně, v rozsahu doporučeném ITIL
MZe	Ministerstvo zemědělství – Česká republika
Maintenance	Služby a aktivity, poskytované výrobcem Systému nebo jeho komponent, potřebné pro udržení Systému v provozuschopném stavu v souladu s dohodnutými parametry a zajišťující kompatibilitu Systému s komponentami ICT Objednatele
Firewall	Zařízení nebo řešení pro řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti
Objednatel, Zadavatel	osoba, která je jako Objednatel definovaná v záhlaví Smlouvy
AAA	Autentizace – Autorizace – Acounting (Auditing), tedy ověření identity - přidělení oprávnění – vytvoření záznamu o přístupu
LDAP	Lightweight Directory Access Protocol - protokol pro ukládání a přístup k datům na adresářovém serveru nebo přímo zkratka pro adresářový server
OS	Operační systém
DB	Databáze
SSL	Secure Sockets Layer - vrstva která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran
Rozhraní Systému	integrační a komunikační rozhraní Systému prezentované vnějším

	rozhraním hraničního (posledního) aktivního síťového prvku pod správou Zhotovitel/Dodavatele, tvořícího rozhraní mezi sítí Zhotovitel/Dodavatele a vnější komunikační infrastrukturou
Servisní okno	časový interval definovaný Objednatelem a zakotvený v dokumentaci, pro potřeby odstávek
SIEM	Security incident & event management – systém pro správu incidentů a událostí
Smlouva	Smlouva o poskytnutí řešení „Systém“ uzavřená mezi Objednatelem a Zhotovitel/Dodavatelem
Standardní SW (SSW)	softwarové vybavení třetích stran dodané v rámci Smlouvy, na základě kterého byl zhotoven Systém, které nebylo vyvinuto Zhotovitel/Dodavatelem a není aplikační SW komponentou Systému vyvinutou v rámci Smlouvy
Systém	Vyvíjená nebo vyvíjená a dodávaná aplikace, informační systém na míru nebo podobný program a řešení, a dále i komerční software
Zhotovitel/Dodavatel	osoba, která je jako Zhotovitel/Dodavatel definovaná v záhlaví Smlouvy