Príloha č. 2

KANCELÁRIA NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

Verzia dokumentu	1.0
Dátum vydania	
Názov dokumentu	Smernica požiadavky na bezpečný vývoj a SSDLC
Gestor	
Vlastník	Kancelária NR SR

Obsah

Prílohy:

Príloha č. 1 - Požiadavky na bezpečný návrh web aplikácií – viď. aj samostatný xls dokument "Bezpečnostné požiadavky audit checklist", záložka "Audit checklist webapp"

Príloha č. 2 - Požiadavky na bezpečný návrh aplikácií – viď. aj samostatný xls dokument "Bezpečnostné požiadavky audit checklist", záložka "Audit checklist bezp"

Článok 1 Úvodné ustanovenia

1) Politika informačnej bezpečnosti KNR SR rozpracováva strategické smerovanie riešenia kybernetickej bezpečnosti a stanovuje rámec systému riadenia bezpečnosti pre informačné a komunikačné systémy KNR SR. Jednou z požiadaviek na aplikovanie bezpečnostných opatrení je vytvorenie požiadaviek na vývoj aplikácií a informačných systémov. Metodika je vytvorená na základe vybraných častí odporúčaní a zverejnených metodík CSIRT SK (www.csirt.gov.sk) NUKIB CZ (https://www.nukib.cz), CISA.GOV a NIST. Tieto boli doplnené resp. aktualizované pre potreby spoločnosti KNR SR.

Článok 2 Bezpečnosť životného cyklu IS a SSDLC

1) Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôsobiť tomu projektovanie, návrh aj implementáciu samotného riešenia počas jednotlivých fáz. Rozsah jednotlivých fáz môže pre daný konkrétny prípad (aplikáciu alebo projekt) z pohľadu bezpečnosti meniť garant informačnej bezpečnosti v spolupráci s vedúcim OISPESaBIKT.
2) V prípade vývoja aplikácií alebo informačných systémov je nevyhnutné zohľadniť požiadavky platnej legislatívy SR a EÚ (napríklad Nariadenie 2016/679 GDPR, najmä recitál (49) a (78)) pre všetky dotknuté informačné systémy alebo aplikácie.
3) Pokiaľ je to možné, je potrebné aplikovať požiadavky dobrej praxe, najmä SSDLC (Secure Software Development Life Cycle) (viď. popis nižšie).
4) SSDLC je model riadenia bezpečnosti vo vývoji informačných systémov a aplikácií, ktorý pozostáva z niekoľkých fáz.
5) Tento model musí byť aplikovaný pri každej významnej zmene IS v rámci procesu riadenia zmien (Smernica Riadenie zmien), a musí byť vyžadovaný pre všetky systémy ktoré budú spadať do kategórie „kritický informačný systém“ alebo budú mať zásadný vplyv na chod kritických systémov alebo procesov organizácie.
6) O výnimkách z aplikovania jednotlivých fáz SSDLC rozhoduje vedúci OISPESaBIKT a garant informačnej bezpečnosti. V prípade sporu rozhoduje bezpečnostná komisia KNR SR.
7) Stručné zhrnutie fáz SSDLC:
    - Fáza inicializácie (článok 3)
        - Špecifikácia systémových požiadaviek
        - Určenie bezpečnostných požiadaviek (hlavné zásady uvedené v článku 4)
        - Hodnotenie bezpečnostných vlastností
        - Analýza zhody bezpečnostných opatrení medzi zadávateľom a dodávateľom
    - Fáza dizajnu a vývoja/obstarania (článok 5)
        - Dizajn systému
        - Stanovenie bezpečnostných požiadaviek pre fázu dizajnu
        - Analýza a modelovanie hrozieb
        - Vývoj alebo obstaranie
    - Fáza testovania a verifikácie (článok 6)

- Verifikácia efektívnosti nasadených bezpečnostných mechanizmov
- Manažment zraniteľností
- Reporting
- Bezpečnostné testy
    - Preskúmanie konfigurácie
    - Skenovanie zraniteľností
    - Audit pravidiel firewallov
    - Testy procesov záloh a obnovy zo záloh
    - Testovanie obnovy systémov po výpadku
    - Testovanie aplikovania bezpečnostných záplat systémov
    - Testovanie aktualizácií bezpečnostných komponent
    - Testovanie bezpečnosti prístupov, vrátanie overovania prihlasovania a vzdialených prístupov
- Penentračné testy, technologické audity a skenovanie
- Reporting

- Fáza implementácie/ohodnotenia bezpečnostných charakteristík (článok 7)
    - Implementácia bezpečnostných požiadaviek na systém
    - Implementácia bezpečnostných požiadaviek prostredia (ekosystému – prepojenie na okolité systémy v prostredí)
    - Bezpečnostný hardening systémov
    - Riadenie zmien
- Fáza nasadenie a prevádzka riešenia (článok 8)
    - Odovzdanie systému do prevádzky
    - Bezpečnostný monitoring a monitoring implementovaných opatrení
    - Overovanie odovzdávanej dokumentácie (systémová, prevádzková, používateľské príručky, bezpečnostné analýzy a audity)
    - Zaškolenie administrátorov a používateľov systémov
    - Prevádzka systému
    - Prevádzkový a bezpečnostný monitoring
    - Pravidelné bezpečnostné testovanie, bezpečnostné analýzy, audity a pentesty
    - Bezpečnostné aktualizácie komponent a aplikovanie bezpečnostných záplat
    - Zmenové konanie a vydanie nových verzií
- Fáza odstránenia/vyradenia (článok 9)
    - Príprava a ukončenie zmluvných vzťahov, licencií a pod.
    - Bezpečné odstavenie systému
    - Archivácia nevyhnutných údajov
    - Bezpečná likvidácia informácií
    - Reporting o vyradení systému

Článok 3 Fáza inicializácie

1) Počas tejto fázy v organizácii vzniká potreba pre určitý systém a organizácia dokumentuje jeho požadovaný účel. Organizácia na globálnej úrovni typicky vyhodnocuje informácie, ktoré bude systém spracovávať, prenášať alebo uchovávať takisto kto bude požadovať prístup k informáciám a ako.
2) V tejto fáze sa rozhodne či sa projekt bude realizovať ako nezávislý informačný systém alebo sa vytvorí ako súčasť už existujúceho definovaného systému. Ďalej sa v tejto fáze typicky vykoná predbežná analýza rizík a začnú sa vypracovávať dokumenty bezpečnostných plánov systému.
3) Ak sa ukončia vyššie uvedené činnosti a bola uznaná potreba pre nový alebo vylepšený produkt IT alebo službu, ešte predtým než sa projekt schváli, musia byť vykonané ďalšie činnosti, ktoré zahrňujú jasne definované ciele projektu a definovanie globálnych požiadaviek na informačnú bezpečnosť.
4) Typicky v tejto fáze organizácia definuje globálne požiadavky na politiku informačnej bezpečnosti a definuje architektúru bezpečnostného systému organizácie.
5) Súčasťou tejto fázy je aj:
    a. Špecifikácia systémových požiadaviek
    b. Určenie bezpečnostných požiadaviek
    c. Hodnotenie bezpečnostných vlastností
    d. Analýza zhody bezpečnostných opatrení medzi zadávateľom a dodávateľom
6) Tento proces je taktiež súčasťou procesu riadenia zmien.

Článok 4 Bezpečnostné zásady pri návrhu riešenia

1) Navrhnuté riešenie musí mať modulárnu štruktúru, pričom:
    a. Pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege t.j. používatelia, správcovia systémov a tretie strany musia mať prístup iba k údajom/aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú.
    b. Architektúra riešenia by mala byť viacvrstvová a jednotlivé vrstvy (napr. prezentačná, aplikačná a databázová) majú byť oddelené,
    c. Odporúčané je použitie overených návrhových vzorov, napr MVC, resp. MVP.
2) Interná štruktúra spracovania, vstupné a výstupné funkcie aplikácií, informačných systémov a služieb KNR SR musia byť navrhnuté a vytvorené tak, aby bol proces spracovania informácií v týchto systémoch bezpečný a aby sa vylúčilo riziko
    a. chybného spracovania,
    b. prerušenia prevádzky,
    c. neoprávneného prístupu,
    d. zneužitia a úniku informácií alebo
    e. inej kompromitácie systému.

3) Musia byť identifikované všetky súčasti systému (interné aj externé), od ktorých závisí riešenie. Pre jednotlivé súčasti musia byť identifikované zraniteľnosti, ktoré sa v nich môžu vyskytnúť a vyhodnotiť riziká zneužitia týchto zraniteľností na základe:
    a. prístupového vektoru útočníka (lokálny prístup/sieť),
    b. náročnosti získania prístupu,
    c. potreby autentifikácie,
    d. dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.
4) Na základe analýzy rizík musia byť navrhnuté opatrenia, ako predchádzať možným incidentom a ako postupovať v prípade vzniku incidentu. Tieto opatrenia musia byť zapracované v návrhu riešenia.
5) Za vykonanie analýzy rizík je zodpovedný garant informačnej bezpečnosti. V prípade vykonania analýzy rizík nezávislou externou entitou, túto schvaľuje garant informačnej bezpečnosti a vedúci OISPESaBIKT, po zvážení môžu predložiť analýzu rizík na schválenie bezpečnostnej komisii.

Článok 5 Fáza vývoja/zaobstarania

1) Počas tejto fázy je systém navrhnutý, kúpený, naprogramovaný, vyvinutý alebo inak skonštruovaný. Táto fáza často pozostáva z ďalších definovaných cyklov, ako je cyklus vývoja systému alebo cyklus zaobstarania systému.
2) Počas prvej časti fázy vývoja/zaobstarania systému by organizácia mala súčasne upresniť a následne implemetovať požiadavky na bezpečnosť systému a na funkcionalitu systému. Tieto požiadavky môžu byť vyjadrené ako technické charakteristiky (napríklad riadenie prístupu), záruky (napríklad kvalifikácia a prax vývojárov systému) alebo prevádzkové pravidlá (napríklad bezpečnostné povedomie a školenie).
3) Počas poslednej časti tejto fázy sa zrealizuje vývojové testovanie technických a bezpečnostných charakteristík/funkcií s cieľom ubezpečiť sa, že sa vykonávajú tak ako je zamýšľané, a to ešte predtým ako projekt prejde do nasledujúcej fázy.
4) Hlavné bezpečnostné aktivity pre túto fázu sú:
    a. Navrhnúť bezpečnostnú architektúru.
    b. Vykonávať ohodnotenie rizík a výsledky použiť na doplnenie základných bezpečnostných opatrení.
    c. Vykonať funkčné a príslušné bezpečnostné testy v rámci tejto fázy.
    d. Pripraviť prvotné dokumenty pre certifikáciu a akreditácie systému.
5) Všeobecné typy kontrolných bodov pre túto fázu môžu obsahovať:
    a. Posúdenie architektúry/návrhu, ktoré vyhodnotí plánovaný návrh systému a možnú integráciu s ďalšími systémami, rovnako ako aj začlenenie zdieľaných služieb a spoločných bezpečnostných opatrení takých ako sú napríklad autentizácia, zotavenie po havárii, detekcia prienikov alebo hlásenie incidentov.
    b. Posúdenie výkonnosti systému, ktoré vyhodnotí, či systém prináša alebo bude schopný prinášať dokumentované očakávania majiteľa a či sa systém chová predvídateľným spôsobom v prípade, že je vystavený nesprávnemu používaniu. (Napríklad schopnosť systému udržiavať dostupnosť a integritu údajov pri očakávanom extrémnom zaťažení zdroja).
    c. Preskúmanie funkcionality systému, ktoré zaisťuje dostatočnú detailnosť a testovateľnosť identifikovaných funkčných požiadaviek.

d. Preskúmanie vecného a finančného stavu riešenia projektu je dôležité na odhalenie významných posunov v plánovanej úrovni postupu prác s cieľom zaistiť, že pomer nákladov a prínosov je sledovaný a rozhodnutia sú naďalej účinné.

e. Môže byť potrebné pokračujúce preskúmanie rozhodnutí o manažmente rizika v prípade ak, vzhľadom na vyššie uvedené výsledky preskúmania, sa zmenil systém a/alebo jeho bezpečnostné opatrenia a/alebo jeho požiadavky.

6) Hodnotenie rizík systému

a. Musia sa vziať do úvahy všetky súvisiace platné zákony, vyhlášky a štandardy týkajúce sa riadenia rizík v informačných systémoch.

b. Účelom hodnotenia rizík je zhodnotiť doterajšie znalosti o návrhu systému, stanovených požiadavkách a minimálnych bezpečnostných požiadavkách odvodených v procese bezpečnostnej kategorizácie na stanovenie ich účinnosti pri zmiernení predpokladaných rizík. Výsledky by mali ukázať, že špecifické bezpečnostné opatrenia poskytujú primeranú ochranu alebo upozorniť na oblasti, kde je potrebné ďalšie plánovanie. Pre dosiahnutie úspechu je potrebná účasť ľudí majúcich vedomosti z odborov v rámci domény informačného systému (napríklad používateľov, technických expertov, prevádzkových odborníkov).

c. Hodnotenie bezpečnostných rizík by malo byť vykonané pred schválením špecifikácií návrhu, pretože by mohlo vyústiť do ďalších upresnení alebo poskytnúť ďalšie zdôvodnenia navrhovaných riešení.

d. Okrem toho, vzhľadom na bezpečnostné aspekty vyvíjaného/zaobstarávaného systému by organizácia mala tiež zvážiť to, ako systém môže mať vplyv na iné systémy, s ktorými bude priamo alebo nepriamo prepojený. To môže znamenať, že existujú pôsobiace zdedené spoločné opatrenia alebo existujú ďalšie riziká, ktoré treba zmierniť. V týchto prípadoch môže byť potrebné preskúmanie organizácie na zabezpečenie komplexnejšieho pohľadu na hrozby a zraniteľnosti.

7) Nižšie uvedené zásady musia byť pri vývoji riešenia aplikované podľa danej situácie, pričom rozsah pre daný prípad schvaľuje garant informačnej bezpečnosti a vedúci OISPESaBIKT, v prípade sporu rozhoduje Bezpečnostná komisia.

8) Sumarizácia hlavných zásad, ktoré majú byť pri vývoji uplatňované:

- Pred začiatkom vývoja sa zváži výber použitého jazyka a frameworku z hľadiska bezpečnosti. Keď prebieha voľba použitého jazyka a frameworku, jedným zo zvažovaných bodov by mala byť taktiež bezpečnosť použitých technológií. Z tohto pohľadu je vhodné preferovať moderné jazyky, ktoré minimalizujú problémy so zraniteľnosťami na úrovni pamäte (bez manuálneho uvoľňovania pamäte) a súbehov.
- Pri výbere frameworku je vhodné preferovať tie, ktoré spĺňajú pravidlá pre bezpečné API.
- Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí.
- Vývojové prostredie musí byť oddelené od testovacieho prostredia.
- Účty vývojárov pri autentizácii by mali používať viacfaktorovú autentizáciu.
- Kryptografické podpisovanie jednotlivých zmien kódu je odporúčané.
- V aplikácii alebo informačnom systéme by mali byť použité dôveryhodné (a zároveň široko rozšírené) frameworky/knižnice, ktoré kladú dôraz na bezpečnosť a predchádzanie bežným programátorským chybám a zároveň často a rýchlo zverejňujú opravy bezpečnostných chýb.
- V prípade, že implementované riešenie potrebuje spracovávať dôverné údaje (napr. osobné údaje), počas vývoja aj testovania musia byť použité anonymizované, resp. fiktívne údaje.
- V prípade, že má aplikácia rôzne rozhrania (API), všetky funkcionality okrem verejných (public) častí, by mali vyžadovať autentifikáciu.

- Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie, pričom:
    a. jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
    b. commity by mali mať zmysluplné popisy,
    c. mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.
- Nemali by byť použité funkcie/volania/nástroje, respektíve koncepty, ktoré sú podľa oficiálnej dokumentácie v súčasnej dobe zastarané (deprecated) alebo nebezpečné (unsafe) a mali by byť nahradené odporúčanými alternatívami.
- Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:
    a. zapnuté všetky varovania a ochrany vývojových nástrojov
    b. varovania vývojového prostredia
    c. Všetky varovania z predchádzajúceho bodu by mali byť opravené.
- Aplikácie a knižnice využívajú udržiavané závislosti.
- Ak je využitá externá závislosť, musia byť použité iba knižnice a ich verzie, ktoré sú udržiavané, aby sa znížilo riziko použitia knižnice, ktorá obsahuje zraniteľnosti, ktoré nikto nebude riešiť. Ak aplikácia závisí od neudržovanej knižnice, mala by byť nahradená novšou, podporovanou verziou alebo jej udržiavanou alternatívou.
- Pri výbere knižnice by mali byť preferované tie, ktorých autori dbajú na bezpečnosť vývoja.
- Znaky knižnice, pri ktorých autori dbajú na bezpečnosť:
    a. Je vykonávaná kontinuálna integrácia (CI),
    b. repozitár obsahuje súbor SECURITY, pričom tento súbor je štandardný spôsob informovania uživateľov a bezpečnostných analytikov, a ako majú byť hlásené bezpečnostné chyby, pre hlásenie chýb musí byť využitý neverejný kanál (buď neverejné issues v rámci nástroja na zdieľanie kódu alebo napríklad e-mailový kontakt so zverejneným verejným šifrovacím kľúčom (napr. PGP)).
    c. verejný zoznam nahlásených Issues neobsahuje neopravené nahlásené zraniteľnosti,
    d. súbor CHANGELOG obsahuje nájdené bezpečnostné zraniteľnosti,
    e. oprava nahlásených bezpečnostných chýb trvá menej ako 30 dní,
    f. nájdené zraniteľnosti nie sú triviálneho charakteru (prípadne nie sú obvyklé),
    g. v rámci hľadania zraniteľností autori používajú techniku fuzzingu, respektíve testovanie na vstupy do aplikácie.
- Aplikácie pri definovaní závislostí používajú „lock file", pričom tento je spravidla používaný pri vytváraní uzamknutých (locked) súborov.
- Aplikácia špecifikuje presné verzie závislostí, s ktorými bola testovaná, pokiaľ to daný správca závislostí umožňuje. Cieľom je zabrániť využitiu novšej a potenciálne podvrhnutej verzie závislostí, kedy útočník získa prístup k účtu správcu knižnice a nahradí ju podvrhnutou verziou.
- V prípade webovej aplikácie, ktorá načíta knižnice z externých serverov (CDN) je na tento účel možné použiť technológiu SRI (Subresource Integrity) podporovanú v moderných webových prehliadačoch.
- Závislosti sú sťahované z dôveryhodných úložísk.
- Pri výbere správcov závislostí sú preferovaní takí, ktorí kontrolujú integritu sťahovaného balíčka pomocou podpisu tvorcu aplikácie alebo aspoň pomocou hash-u. Pokiaľ správca závislostí kontrolu

integrity neumožňuje, závislosti sú výhradne sťahované pomocou zabezpečeného kanála (HTTPS, SSH a pod.).

- Vykonáva sa kontrola existencie špecifických reťazcov obsahujúcich prístupové údaje (napr. heslá, tokeny, ssh kľúče – nazývané aj „secrets“) v zdrojovom kóde.
- V rámci kontinuálnej integrácie je použitý nástroj, ktorý detekuje, či zdrojový kód neobsahuje známe súbory alebo reťazce, ktoré obsahujú prístupové údaje (napr. heslá, tokeny pre prístup, súkromné SSH kľúče, certifikáty so súkromným kľúčom a pod.) v angličtine označované ako „secrets ”.
- Sú využívané overené kryptografické knižnice.
- Sú využívané odolné kryptografické prostriedky.
- Je vykonávané overovanie použitého certifikátu, kontrolované aspoň:
    a. či je podpísaný dôveryhodnou certifikačnou autoritou,
    b. či nie je vypršaný alebo naopak pred dobou platnosti,
    c. či Common Name alebo Alternative DNS Names zodpovedá použitej doméne.
- Musia byť stanovené limity pre odstraňovanie zraniteľností. Požiadavky na odstránenie zraniteľnosti sú spravidla stanovené na max. 30 dní.
- Všetky nájdené a nahlásené zraniteľnosti musia byť opravené do stanoveného limitu, vrátane vydania novej verzie opravujúcej túto chybu. Lehota môže byť predĺžená v prípade zraniteľností, ktoré vyžadujú napr. zmenu architektúry aplikácie.
- V prípade kritickej zraniteľnosti (napr. RCE zneužiteľné bez potreby autentizácie, CVSS vyššia ako 9.0) by mala byť oprava do kódu začlenená v rámci hodín pred vydaním novej verzie.
- Všetky zraniteľnosti nájdené aj nahlásené, napr. interným penetračným testom či kontrolou kódu vývojárom, musia byť uvedené v súbore popisujúce vykonané zmeny v jednotlivých verziách (typicky súbor CHANGELOG), ktorý je súčasťou repozitára.
- Ak systém alebo aplikácia využíva relačnú databázu na ukladanie dát a návrh databázovej schémy je súčasťou aplikácie, nasledovné pravidlá musia byť uplatňované na zabezpečenie integrity ukladaných dát a jednoduchšej prenositeľnosti dát do iných systémov:
    a. sú využívané primárne kľúče,
    b. sú používané cudzie kľúče pri väzbe na číselníkové hodnoty alebo na iné entity,
    c. v rámci databázy sú kontrolované hodnoty parametrov („constraints”),
    d. pokiaľ databázový stĺpec predpokladá unikátnu hodnotu, je využitý unikátny index,
    e. pri vkladaní dát sú využívané transakcie,
    f. databázová schéma je komentovaná.
- Počas vývoja musí byť vedená vývojárska dokumentácia:
    a. dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii,
    b. v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená KNR SR.
- Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané KNR SR spolu so samotným riešením.
- Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje (citlivé informcie alebo osobné údaje), autentifikačné údaje musia byť uložené iba v podobe tzv. osolených hashov (salted hash), pričom použitá hashovacia funkcia by mala byť minimálne sha256, ostatné osobné údaje (adresy,

čísla platobných kariet, čísla občianskych preukazov,...) je odporúčané neukladať v čistej podobe, ale chránené šifrovaním.

- Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:
    a. prihlásenie a odhlásenie (úspešné aj neúspešné),
    b. vytvorenie (úspešné aj neúspešné), modifikácia alebo zmazanie používateľa alebo skupiny,
    c. pokusy (úspešné aj neúspešné) pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie),
    d. pokusy o kritické operácie (úspešné aj neúspešné),
    e. v žiadnej úrovni logovania nie sú do log záznamov vkladané tajné identifikátory (heslá, prístupové tokeny, privátne kľúče a pod.).
- Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov alebo podľa súvisiacej platnej legislatívy (GDPR, Registratúra a pod.).
- Riešenie musí podporovať aj logovanie vo formáte protokolu syslog a musí podporovať preposielanie týchto logov na externý syslog server.

Článok 6 Fáza testovanie a verifikácia riešenia

1) Testovacie prostredie musí byť oddelené od predprodukčného prostredia.
2) Predprodukčným prostredím sa rozumie testovanie riešenia pripraveného na nasadenie, pričom sa verifikujú závislosti na prostredí, do ktorého bude riešenie nasadzované. Predprodukčné prostredie musí byť oddelené od ostatných produkčných systémov a riešení.
3) Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:
    - Vývojári alebo testeri overia napr. pomocou automatizovaných nástrojov štandardné zraniteľnosti, prebehne minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leak, memory corruption).
    - Verifikácia efektívnosti nasadených bezpečnostných mechanizmov.
    - Musí byť overený manažment zraniteľností.
    - Vývojári alebo testeri musia zabezpečiť overenie realizácie opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia.
    - Musia byť vykonané príslušné bezpečnostné testy ako:
        a. Preskúmanie konfigurácie.
        b. Skenovanie zraniteľností.
        c. Audit pravidiel firewallov.
        d. Testy procesov záloh a obnovy zo záloh.
        e. Testovanie obnovy systémov po výpadku.
        f. Testovanie aplikovania bezpečnostných záplat systémov.
        g. Testovanie aktualizácií bezpečnostných komponent.
        h. Testovanie bezpečnosti prístupov, vrátanie overovania prihlasovania a vzdialených prístupov.

- Musí byť vykonané penetračné testovanie, najvhodnejšie externou organizáciou.
- Zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

4) Po ukončení verifikácie a testovania sa riešenie testuje v predprodukčnom prostredí, pričom sa verifikujú vzťahy a závislosti na iných informačných systémoch, respektíve nasadenie riešenia do celkového ekosystému organizácie.
5) Ako záznam testovaní ako aj verifikácii musí byť vyhotovený bezpečnostný report. Za analýzu reportu je zodpovedný vedúci OISPESaBIKT.
6) Previerky návrhu a testy systémov musia byť vykonané predtým ako je systém nasadený do prevádzky, aby sa zaistilo, že systém spĺňuje všetky požadované (aj bezpečnostné) špecifikácie.
7) Rovnako sa posudzuje vplyv a integrácia systému na prostredie, do ktorého bude systém alebo aplikácia nasadený (vplyv na ekosystém, okolité informačné systémy). Táto časť testov sa preto realizuje v určenom testovacom (napr. integračnom) alebo v inom, napr. v tzv. predprodukčnom prostredí.
8) Pokiaľ sú do aplikácie alebo podporného systému dodatočne pridané úpravy, musí byť vykonaný dodatočný akceptačný test týchto zmien. Takýto prístup zaisťuje, že dodatočné úpravy spĺňajú stanovené (aj bezpečnostné) špecifikácie a nie sú v konflikte alebo neblokujú existujúce riešenie.
9) Výsledky previerok návrhu a testovania systému musia byť plne dokumentované, prípadne aktualizované po vykonaní nových previerkach a testoch. S týmito dokumentmi by sa malo zaobchádzať ako s oficiálnymi dokumentmi spoločnosti.

Článok 7 Fáza implementácie/ohodnotenia bezpečnostných charakteristík

1) V tejto fáze organizácia konfiguruje a zavádza bezpečnostné charakteristiky systému, testuje funkčnosť týchto charakteristík a nakoniec organizácia udelí oficiálnu autorizáciu na prevádzku systému.
2) Tieto činnosti sa realizujú v určenom testovacom (napr. integračnom) alebo v inom, napr. v tzv. predprodukčnom prostredí. Ide o konfiguráciu a zavádzanie bezpečnostných požiadaviek v celom prostredí (v celom ekosystéme, s prepojením na okolité systémy v prostredí).
3) Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní o bezpečnej prevádzke služieb a infraštruktúry, ktoré v rámci Iniciačnej fázy poskytne KNR SR.

Článok 8 Fáza nasadenie a prevádzka riešenia

1) Fáza odovzdania do prevádzky pozostáva v oficiálnom prevzatí diela a akceptácii prác.
2) Je overované formálne zaznamenanie vlastníkov a správcov informačných systémov.
3) Súčasťou prevzatia systémov je aj overovanie odovzdávanej dokumentácie (systémová, prevádzková, používateľské príručky, bezpečnostné analýzy a audity), túto overuje garant informačnej bezpečnosti,

vedúci OISPESaBIKT, riaditeľ OIaKT, vlastník a prípadne ďalšie delegované osoby za stranu KNR SR (administrátor, bezpečnostný administrátor a pod.).

4) Nevyhnutnou súčasťou tejto fázy je aj zaškolenie administrátorov a používateľov systémov, zaškolenie je zaznamenané minimálne v prezenčných listinách, alebo v prípade online, inou verifikáciou, že školenie bolo absolvované. Nedostatočné porozumenie fungovania systému má za následok ako chybovosť, tak aj zníženie bezpečnosti systémov.
5) Súčasťou tejto fázy je taktiež spustenie kompletného navrhnutého bezpečnostného monitoringu systémov ako aj monitoringu implementovaných opatrení. V prípade začlenenia výstupov do centrálneho monitorovacieho systému sa overuje funkčnosť prepojenia týchto systémov, ak tak z prevádzkových dôvodov nebolo urobené v predchádzajúcej fáze.
6) Účinný bezpečnostný program vyžaduje komplexnú a neustálu znalosť programu a poznanie slabín systému.
7) Vo fáze prevádzky a údržby sú systémy a produkty nasadené v prevádzke, vyvíjajú a testujú sa vylepšenia a modifikácie systému a pridáva sa alebo sa nahradzuje hardvér a softvér.
8) Počas tejto fázy by organizácia mala permanentne monitorovať výkon systému, aby sa zaistilo, že systém vyhovuje stanoveným požiadavkám používateľov a bezpečnosti a že sú zapracované potrebné modifikácie systému.
9) Pre riadenie a manažment konfigurácií je dôležité dokumentovať navrhnuté a uskutočnené zmeny v bezpečnostnom pláne systému. Informačné systémy sú typicky v neustálom stave vylepšovania či už hardvéru alebo softvéru alebo možných zmien okolitého prostredia, v ktorom je systém umiestnený. Dokumentovanie zmien v informačnom systéme a vyhodnotenie potenciálneho dopadu týchto zmien na bezpečnosť systému je podstatnou časťou priebežného monitorovania.
10) Monitorovanie bezpečnostných opatrení napomáha identifikovať potenciálne problémy informačného systému vo vzťahu k bezpečnosti, ktoré neboli identifikované počas analýzy bezpečnostných dopadov vykonávanej ako časť procesu riadenia a manažmentu konfigurácií.
11) Musí byť preto zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami.
12) Musí byť taktiež zabezpečené pravidelné bezpečnostné testovanie, bezpečnostné analýzy, vykonávanie auditov a penetračných testov.
13) Bezpečnostné aktualizácie komponent a aplikovanie bezpečnostných záplat musí podliehať opatreniam uvedeným v Smernici práva a prevádzka informačných systémov a služieb a smernici o riadení zmien, ktoré poskytne KNR SR v rámci iniciačnej fázy.

Článok 9 Fáza odstránenia

1) Fáza odstránenia životného cyklu systému odpovedá procesu zachovania (ak sa aplikuje) a zničenia informácií, hardvéru a softvéru informačného systému.
2) Tento krok je mimoriadne dôležitý, pretože počas tejto fázy sú informácie, hardvér, softvér prenesené na iný systém alebo sú archivované alebo zničené. Ak je táto fáza vykonaná nesprávne, táto skutočnosť môže mať za následok napríklad neoprávnené zverejnenie citlivých údajov.
3) Ak sa informácie archivujú, musí organizácia brať na zreteľ potrebu a metódy znovu sprístupnenia informácií. Aj keď elektronické informácie je relatívne jednoduché uložiť a znovu sprístupniť, môžu nastať

problémy, pokiaľ technológia použitá na vytvorenie záznamov nebude v čase znovu pristúpenia k informáciám dostupná v dôsledku zastaranosti alebo nekompatibility s novými technológiami.

4) Neoddeliteľnou súčasťou je aj analýza a príprava na korektné ukončenie zmluvných vzťahov, licencií a pod. s ohľadom na platnú legislatívu SR a EÚ. Príprava na ukončenie musí prebiehať v adekvátnych termínoch tak, aby boli všetky stanovené zmluvné a legislatívne podmienky splnené.

5) Súčasťou tejto fázy je zabezpečenie bezpečného odstavenia systému tak, aby bola zachovaná kontinuita všetkých dotknutých procesov, pričom sa berie ohľad na okolité informačné systémy v ekosystéme (ak existujú), analyzujú sa väzby na tieto procesy a systémy, pričom musí byť zachovaná ich integrita a musí byť zabezpečené, aby ich bezpečnosť nebola dotknutá alebo znížená.

6) Navyše organizácia KNR SR musí brať do úvahy opatrenia, ktoré musia byť realizované pre budúce použitie šifrovaných údajov. Opatrenia sa týkajú zaistenia dlhodobého bezpečného uloženia kryptografických kľúčov. Pri odstavení informačného systému je rovnako dôležité brať do úvahy právne požiadavky na dobu archivácie údajov respektíve Registratúrny plán organizácie.

7) Je nevyhnutné zabezpečiť bezpečnú likvidáciu všetkých citlivých informácií a osobných údajov, teda odstránenie informácií z pamäťového média ako je pevný disk alebo magnetická páska (tzv. sanitácia médií). Existuje viacero úrovní bezpečnosti pri sanitácii médií - od obyčajného vymazania informácií cez bezpečnostné zmazanie informácií až po fyzické zničenie média. Vzhľadom k tomu, že existuje viacero typov sanitácie médií poskytujúcich rôznu ochranu informáciám, organizácia KNR SR má mať stanovené bezpečnostné požiadavky vo forme smernice na výber sanitačnej metódy. Bližšie informácie sú dostupné v smernici klasifikácia a ochrana informačných aktív, ktorú celú alebo jej časť poskytne KNR SR pred fázou odstránenia.

8) Fázu odstránenia je potrebné realizovať v súlade so smernicou o riadení zmien.

9) Záverečnou činnosťou je vytvorenie reportu o vyradení systému, ktorý vypracúva vedúci OISPESaBIKT.

Článok 10 Záverečné ustanovenia

1) Za obsah a aktualizáciu tejto smernice, vrátane príloh, zodpovedá garant informačnej bezpečnosti KNR SR.

2) Táto smernica musí byť revidovaná najmenej jedenkrát za pol roka, alebo pri každej významnej zmene v štandardoch bezpečného vývoja aplikácií a software, alebo bezpečnostných protokoloch (napríklad požiadavka na vyššiu verziu protokolu TLS).

POŽIADAVKY PRE TRETIE STRANY

BEZPEČNOSTNÉ OPATRENIA

KANCELÁRIE NÁRODNEJ RADY SLOVENSKEJ REPUBLIKY

Obsah

Úvodné ustanovenia

„Bezpečnostná politika kybernetickej bezpečnosti“ rozpracováva strategické smerovanie riešenia kybernetickej bezpečnosti a stanovuje rámec systému riadenia bezpečnosti pre informačné a komunikačné systémy **Kancelárie Národnej rady Slovenskej republiky** so sídlom Námestie Alexandra Dubčeka 1, 812 80 Bratislava 1 (ďalej ako „Kancelária NR SR “).

Jednou z požiadaviek na aplikovanie bezpečnostných opatrení podľa Zákona č. 95/2019 o Vyhlášky č. 179/2020 ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy a Zákona č. 69/2018 o kybernetickej bezpečnosti (ďalej len „zákon o KB a Vyhlášky č. 362/2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení je vytvorenie požiadaviek na aplikovanie bezpečnostných opatrení pre tretie strany.

Vymedzenie Základných pojmov

1) Na účely tejto smernice sa rozumie:
   a) **aktívum** – všetko, čo má pre Kanceláriu NR SR hodnotu (hardvérové komponenty, softvér, dáta, služby, ľudské zdroje, dobré meno Kancelárie NR SR a pod.),
   b) **analýza rizík** – proces identifikácie bezpečnostných rizík, určenie ich rozsahu a identifikácie oblastí, pre ktoré sú potrebné bezpečnostné opatrenia,
   c) **bezpečnostný incident** – udalosť, ktorej dôsledkom je narušenie bezpečnosti aktíva alebo porušenie bezpečnostnej politiky Kancelárie NR SR,
   d) **bezpečnostné opatrenie** – činnosť, zariadenie, procedúra alebo mechanizmus, ktorý eliminuje alebo minimalizuje možnosti vzniku, pôsobenia a následky bezpečnostného incidentu, hrozby alebo udalosti,
   e) **Bezpečnostná politika** – základný dokument systémového riešenia ochrany všetkých aktív spoločnosti pred možnými hrozbami a rizikami. Bezpečnostnou politikou sa vymedzujú bezpečnostné ciele, bezpečnostné požiadavky a zásady, základné organizačné opatrenia a zodpovednosť za jednotlivé bezpečnostné oblasti,
   f) **dostupnosť** – požiadavka, aby aktívum bolo na požiadavku oprávneného zamestnanca prístupné a schopné použitia,
   g) **dôvernosť** – umožnenie prístupu k IS a ním spracúvaným elektronickým informáciám iba pre určené subjekty,
   h) **Garant informačnej a kybernetickej bezpečnosti** (ďalej len „garant bezpečnosti“ alebo „garant informačnej bezpečnosti))– subjekt zodpovedný za presadzovanie, kontrolu a dodržiavanie celkovej bezpečnosti v Kancelárii NR SR, garant informačnej a kybernetickej bezpečnosti je zároveň manažérom kybernetickej bezpečnosti podľa Zákona o kybernetickej bezpečnosti a Vyhlášky š. 362/2018 §5 písm. a)

i) **Gestor IS** – organizačný útvar, ktorý predkladá požiadavku na verejné obstarávanie za účelom zabezpečenia svojich potrieb; ak je potrebný pre zabezpečenie činností viacerých organizačných útvarom, Gestorom je organizačný útvar, ktorý má najväčší finančný podiel na zákazke,

j) **incident** – akákoľvek udalosť, ktorá nie je súčasťou bežnej prevádzky IS/IKT služby a ktorá spôsobuje, prípadne môže spôsobiť prerušenie alebo pokles v kvalite danej služby,

k) **informačno-komunikačné technológie** (IKT) – integrovaný súbor technológií, používaných na manažovanie informácií, procesov a komunikácie v elektronickej podobe za účelom dosiahnutia účinných a efektívnych výsledkov optimalizovaním manažmentu zdrojov distribúcie informácií a vedomostí; ide napríklad o softvér, hardvér a metódy určené pre zber, spracovanie, prenos a úschovu informácií v dátovej (elektronickej) forme,

l) **informačná bezpečnosť** – súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, integrity a dostupnosti informačných aktív,

m) **informačné aktívum** – aktívum v informačnom prostredí Kancelárie NR SR (znalosti a dáta/informácie, ktoré majú pre Kanceláriu NR SR hodnotu),

n) **integrita** – vlastnosť ochrany správnosti a úplnosti aktíva,

o) **informačný systém (IS)** – funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických a programových prostriedkov, ktoré sú súčasťou informačného systému; ide o súhrn prvkov hardvéru, softvéru, komunikačných a ďalších technológií, používaných pre záznam, uchovanie, prenos a využívanie informácií a dát,

p) **ISO** – International Standard Organization (medzinárodná štandardizačná organizácia),

q) **klasifikované informácie** – informácie, pri ktorých porušenie informačnej bezpečnosti predstavuje neakceptovateľné riziko pre organizáciu,

r) **kontinuita činností** – zabraňuje prerušeniam prevádzkových aktivít a chráni kritické procesy organizácie pred vplyvmi závažných zlyhaní alebo havárií informačných systémov a zabezpečuje ich včasnú obnovu,

s) **kybernetický bezpečnostný incident** - akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému, alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií.

t) **médiá** – nosiče informácií listinného charakteru (papierové dokumenty, tlačové zostavy, systémová dokumentácia a pod.) a nelistinného charakteru (CD, DVD, USB disk, magnetická páska, disketa, vymeniteľný disk a pod.),

u) **ošetrenie rizík** – proces na úpravu rizík,

v) **riadenie rizík** – koordinované aktivity na riadenie organizácie s ohľadom na riziká,

w) **riešiteľ bezpečnostného incidentu** - poverený zamestnanec ktorý je oprávnený riešiť bezpečnostný incident, spravidla garant informačnej bezpečnosti alebo osoba poverená jeho zastupovaním (kapitola 8, odsek č. 3., 7., 9., 10., 11.)

x) **riziko** – miera ohrozenia vyjadrená pravdepodobnosťou vzniku nežiaduceho javu a jeho dôsledkami,

y) **zamestnanec** – je osoba, ktorá vykonáva prácu v prospech Kancelárie NR SR na základe pracovnoprávneho vzťahu.

Bezpečnosť prevádzky

1) Cieľom tejto oblasti je zabezpečenie správnej a bezpečnej prevádzky IS, predchádzanie narušeniu bezpečnosti pri práci s pamäťovými médiami, predchádzanie strate, modifikácii alebo zneužitiu informácií pri ich výmene s okolím Kancelárie NR SR. Ide o nasledovné oblasti:
   a) dokumentácia prevádzkových postupov,
   b) bezpečnosť prenositeľných médií,
   c) riadenie zmien,
   d) riadenie kapacít,
   e) ochrana pred škodlivým softvérom,
   f) zálohovanie a archivácia,
   g) zaznamenávanie dát a monitorovanie,
   h) riadenie prevádzkového softvéru,
   i) riadenie technickej zraniteľnosti.
2) Na zaistenie správneho využívania bezpečnostných mechanizmov sa musí spôsob ich použitia zdokumentovať. Dokumentácia o kritických informačných systémoch Kancelárie NR SR obsahuje:
   a) Používateľskú dokumentáciu,
   b) Administrátorskú dokumentáciu,
   c) Prevádzkovú dokumentáciu.
3) Prevádzkové postupy a dokumentované postupy pre správu systémov sú spracované ako oficiálne dokumenty a ich zmeny autorizuje manažment.
4) Používanie prenosných médií musí byť formálne upravené a je povolené iba pre určené spôsoby použitia.
5) Pri zasielaní údajov mimo Kancelárie NR SR sa musia zohľadniť požiadavky aplikovateľnej legislatívy[1].
6) Zmeny informačných systémov musia byť riadené. Taktiež musí byť zavedený formálny postup schvaľovanie navrhovaných zmien.
7) Pri zmenách v prevádzkovom prostredí nesmie byť podstatným spôsobom narušená prevádzka ani znížená bezpečnosť.
8) Zmeny musia byť testované a musia byť zhodnotené vplyvy takýchto zmien na bezpečnosť IS.

[1] Napr. v súlade s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov (všeobecné nariadenie o ochrane údajov - ďalej v texte len „Nariadenie“) a so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov, Výnosom MF SR č.55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy v znení neskorších predpisov a pod.

9) Musia byť dostupné návratové a havarijné postupy vrátane postupov a zodpovedností za prerušenie, alebo predčasné ukončenie a obnovu z neúspešnej zmeny a nepredpokladaných udalostí.
10) Použitie prostriedkov musí byť monitorované a musia sa vykonávať odhady budúcich požiadaviek na kapacity, z dôvodu zabezpečenia dosiahnutia požadovanej výkonnosti systému.
11) Ochrana informačných systémov Kancelárie NR SR pred škodlivým softvérom je v rozsahu najmenej:
    a) kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
    b) detekcie prítomnosti škodlivého kódu na všetkých zariadeniach informačných systémov Kancelárie NR SR (pracovné stanice, notebooky, externé nosiče a pod.),
    c) kontroly súborov prijímaných zo siete Internet a odosielaných do tejto siete na prítomnosť škodlivého softvéru,
    d) detekcie prítomnosti škodlivého kódu na webových stránkach.
12) Pravidelne sa vytvárajú a testujú záložné kópie dôležitých informácií a softvéru.
13) Pre médiá obsahujúce záložné kópie sa musí zaistiť rovnaký stupeň bezpečnosti, ako je požadovaný pre údaje, ktoré sú na nich uložené. Tieto médiá sa musia zároveň uchovávať mimo priestorov s centrálnymi komponentmi IS tak, aby sa minimalizovalo riziko súčasného poškodenia originálnych aj záložných údajov.
14) Testovanie obnovy informačných systémov Kancelárie NR SR a údajov z prevádzkovej zálohy sa vykonáva najmenej 1x za rok. Testujú sa aj redundantné zapojenia zariadení.
15) Ako prevencia pred zlyhaním IS sa musí využívať monitorovanie v týchto oblastiach:
    a) záťaž kľúčových komponentov IS a komunikačnej infraštruktúry,
    b) kapacitné rezervy kľúčových komponentov IS (napr. voľné miesto na systémovom disku),
    c) výskyt chýb v IS.
16) Záznamy udalostí zaznamenávajúce aktivity používateľov, výnimky a udalosti informačnej bezpečnosti musia byť vytvárané, uchovávané a pravidelne preskúmavané.
17) Informácie obsiahnuté v záznamoch, ako aj prostriedky na ich tvorbu musia byť chránené pred neoprávnenými zásahmi a neautorizovaným prístupom.
18) Aktivity Správcu IS a operátora musia byť zaznamenávané. Záznamy musia byť chránené a pravidelne preskúmavané. Záznamy tretích strán musia byť ukladané na zariadeniach Kancelárie NR SR, ku ktorým musia mať umožnený prístup jej relevantní zamestnanci.
19) Hodiny na všetkých relevantných systémoch na spracúvanie informácií v rámci Kancelárie NR SR musia byť synchronizované prostredníctvom jediného presného časového zdroja.
20) Musia byť zavedené postupy na riadenie inštalovania softvéru na prevádzkových systémoch. Pre inštaláciu softvéru používateľmi musia byť vytvorené a zavedené prísne pravidlá.
21) Informácie o technickej zraniteľnosti využívaných informačných systémov musia byť zhromažďované a zhodnocovaná miera vystavenia sa zraniteľnosti. Následne sa musia zavádzať príslušné opatrenia na potlačenie týchto rizík.
22) Hodnotenie zraniteľností informačných systémov Kancelárie NR SR musí byť vykonávané s periodicitou najmenej raz ročne.

23) Používanie prenosných médií (napríklad USB diskov, USB kľúčov) na prenos informácií súvisiacich výhradne s plnením služobných alebo pracovných povinností je v kancelárii NR povolené.
24) Pri používaní prenosných médií musia používatelia zachovávať primerané bezpečnostné opatrenia, ktoré eliminujú riziko prezradenia, zneužitia alebo neautorizovaného prístupu k citlivým informáciám.
25) Bezpečnostnými opatreniami podľa odseku 24 sú najmä
    a) ochrana média pred stratou alebo krádežou jeho bezpečným skladovaním a prenášaním,
    b) externé prenosné médiá a informácie na nich uložené musia byť chránené šifrovaním s nastavením silného hesla minimálne desať alfanumerických znakov na otvorenie dokumentov, pričom pre šifrovanie sa používa asymetrické šifrovanie s minimálnou dĺžkou kľúča 2048kB,
    c) používanie prenosných médií iba na dôveryhodných počítačoch.
26) Za dodržiavanie bezpečnostných opatrení podľa odseku 25 ako aj za prípadné škody spôsobené zneužitím, prezradením, neautorizovaným prístupom k informáciám uloženým na prenosných médiách zodpovedá ich používateľ.
27) Všetky nepotrebné prenosné médiá vo vlastníctve úradu musia byť zlikvidované bezpečným spôsobom tak, aby nebolo možné z týchto médií extrahovať žiadne citlivé informácie.
28) Za likvidáciu nepotrebných médií podľa odseku 5 je zodpovedné oddelenie IT.
29) Pri manipulácii a prenose informácií musia byť dodržané bezpečnostné opatrenia. Bezpečnostné opatrenia sú uplatňované najmä pri
    a) fyzickom prenose informácií (napríklad dokumentov),
    b) emailovej komunikácii vrátane zasielania príloh,
    c) elektronickom prenose,
    d) prenose, zobrazovaní informácií v informačnom systéme,
    e) používaní mobilných prostriedkov,
        a. telefonickej komunikácii, vrátane zasielania správ,
        b. faxovej komunikácii,
        c. zasielaní rýchlych správ (napríklad Instant Messaging, chat).
30) Pri výmene alebo prenose informácií medzi úradom a tretími stranami musí byť vykonaný odhad možných bezpečnostných rizík a určené bezpečnostné opatrenia na ochranu prenášaných informácií.
31) Vlastník informačného aktíva uzavrie s treťou stranou zmluvu o prenose informácií, ktorá musí obsahovať aspoň ustanovenia o bezpečnostných opatreniach (technologických, procesných, personálnych), ktoré boli určené pre tento prenos ako aj zodpovednosť za ich dodržiavanie.
32) Ucelené bezpečnostné požiadavky a opatrenia sú uvedené v dokumente CSIRT.SK: https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf

Bezpečnosť sieťovej komunikácie

1) Cieľom tejto oblasti bezpečnosti je predchádzať strate, neoprávnenej modifikácii alebo zneužitiu elektronických služieb a elektronických informácií v sieťach a v podporných zariadeniach, ktoré ich v sieti spracúvajú, ako aj ošetriť bezpečnosť prenášaných informácií v rámci organizácie a s ktoroukoľvek treťou stranou.
2) Vonkajšie aj vnútorné sieťové prostredie v Kancelárii NR SR je chránené prostredníctvom technologického riešenia na ochranu perimetra siete.
3) Na pripojenie zariadenia k bezdrôtovej sieti sa vzťahujú rovnaké bezpečnostné požiadavky ako na fyzické pripojenie zariadenia k zóne, ku ktorej je pripojená daná bezdrôtová sieť.
4) Auditné záznamy z aktívnych sieťových zariadení, príslušných serverov sa zaznamenávajú a ukladajú a zálohujú..
5) Kancelária NR SR vedie evidenciu o všetkých miestach prepojenia v sieti vrátane prepojení s externými sieťami.
6) Za účelom ochrany sieťovej infraštruktúry, prenášaných informácií a prepojených informačných systémov a služieb musia byť na úrade realizované bezpečnostné opatrenia.
7) Za realizáciu bezpečnostných opatrení sieťovej infraštruktúry úradu je zodpovedný odbor IT.
8) Bezpečnostné opatrenia sú určené na základe posúdenia bezpečnostných rizík a to najmä ochrany:
    a) prenášaných informácií,
    b) uchovávaných informácií (napríklad dočasných súborov, obsahu uloženého do medzipamätí - cache),
    c) dizajnu sieťovej infraštruktúry,
    d) informácií o konfigurácii sietí, sieťových zariadení, definícií kontroly prístupu, oprávnení, správcovských hesiel a kryptografických kľúčov,
    e) sieťových ciest a trás,
    f) sieťových zdrojov (napríklad šírky pásma),
    g) hranice a obvodu siete,
    h) rozhrania informačného systému do sietí.
9) Konfigurácia sieťových zariadení musí byť zdokumentovaná. Zmeny konfigurácie sieťových zariadení, definícií kontroly prístupu, smerovania a prihlasovacích údajov musia byť zdokumentované a kontrolované.
10) Na sieťových zariadeniach musia byť použité aspoň tieto bezpečnostné opatrenia:
    a. všetky prístupy a konfiguračné zmeny sieťových zariadení musia byť logované,
    b. pre prístup musí byť použitý zabezpečený (šifrovaný) kanál, prípadne viacfaktorová autentifikácia,
    c. konfigurácie zariadení musia byť zálohované bezpečným spôsobom.
11) Ak sú na základe klasifikácie informačných aktív prenášané interné alebo chránené informácie, alebo na základe posúdenia rizík iné citlivé údaje je nutné použiť šifrovanie dát, správ, alebo trasy prenosu (SSH, SSL, TSL, VPN tunel a iné).

12) Pri používaní lokálnych bezdrôtových sietí (Wi-Fi sieť) musia byť použité aspoň tieto bezpečnostné opatrenia:
    a. silné šifrovanie WPA2, WPA3
    b. silné heslo pre pripojenie (minimálne desať znakov),
    c. autentifikácia používateľov,
    d. pri spojení siete s lokálnou sieťou je nevyhnutné použiť zabezpečenie certifikátmi.
13) Ak sa poskytuje bezdrôtová sieť (Wi-Fi) externým subjektom (napríklad konferencie, návštevy), musí byť bezdrôtová sieť oddelená od lokálnej počítačovej siete.
14) Na sieťových zariadeniach musí byť nastavené logovanie a monitorovanie všetkých dôležitých udalostí a to najmä
    a. sieťovej komunikácie odchádzajúcej mimo infraštruktúru úradu,
    b. internej sieťovej komunikácie týkajúcej sa citlivých informácií a informačných systémov,
    c. bezpečnostných incidentov na sieťových zariadeniach ako napríklad prihlásenie a zmena konfigurácie,
    d. bezpečnostných udalostí na systémoch poskytujúcich autentifikačné a autorizačné služby v sieťovej infraštruktúre.
15) Aktivity v informačných systémoch a počítačových sieťach úradu musia byť za účelom odhalenia možného bezpečnostného incidentu monitorované, analyzované a vyhodnocované prostredníctvom ďalších bezpečnostných zariadení (NIDS – Network Intrusion Detection System, SIEM – Security Information and Event Management).
16) Za monitorovanie sieťovej infraštruktúry je zodpovedný odbor IT.
17) Ucelené bezpečnostné požiadavky a opatrenia sú uvedené v dokumente CSIRT.SK: https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf

Nákup, vývoj a údržba IS

1) Za účelom redukcie rizika neakceptovateľného výkonu, alebo zlyhania informačných systémov je potrebné monitorovať kapacitu jednotlivých informačných systémov, zisťovať súlad s požiadavkami na ich výkon, ich kapacitné limity a na tomto základe plánovať a optimalizovať kapacity v dostatočnom predstihu. Za plánovanie, monitorovanie a optimalizáciu kapacít je zodpovedný odbor informačných technológií.
2) Cieľom tejto oblasti bezpečnosti je zabezpečiť integráciu informačnej bezpečnosti do informačných systémov v celom ich životnom cykle a zaistiť, aby IT projekty prebiehali riadeným a bezpečným spôsobom.
3) Riešenie informačnej bezpečnosti Kancelárie NR SR je súčasťou celého životného cyklu IS počínajúc jeho obstarávaním.
4) Pre každý IT projekt, ktorý má byť prevádzkovaný v prostredí Kancelárie NR SR sú identifikované a špecifikované bezpečnostné požiadavky, ktoré sa stávajú súčasťou zadávacej dokumentácie k výberovému konaniu a následne sú premietnuté do zmluvy s dodávateľom.

5) V každom IT projekte je na strane dodávateľa aj na strane Kancelárie NR SR zriadená a obsadená rola zodpovedná za informačnú bezpečnosť. Na strane Kancelárie NR SR za informačnú bezpečnosť zodpovedá Garant bezpečnosti. Táto rola zabezpečuje (v rozsahu svojej pôsobnosti na strane Kancelárie NR SR a na strane dodávateľa):
   a) zohľadnenie právnych predpisov a technologických požiadaviek na bezpečnosť,
   b) integráciu bezpečnostných požiadaviek do IT projektu,
   c) vykonanie analýzy rizík,
   d) špecifikovanie bezpečnostných opatrení a dohľad nad ich implementáciou.
6) Súčasťou každého IT projektu je nevyhnutná analýza rizík a návrh opatrení na ich minimalizáciu, spracovaná vo forme bezpečnostného projektu alebo inej forme bezpečnostnej dokumentácie zohľadňujúcej legislatívu aplikovateľnú na predmetný IS, jeho vývoj a údržbu.
7) Pred vývojom a implementáciou nových IS ovplyvňujúcich existujúce IS v prostredí Kancelárie NR SR musí byť ako súčasť analýzy rizík vykonaná aj analýza dopadov zmien na už prevádzkované IS a ich služby. V prípade identifikácie nepokrytých rizík musia byť navrhnuté a implementované dodatočné bezpečnostné opatrenia.
8) Súčasťou každého IT projektu je vytvorený návrh formy výkonu a rozsahu bezpečnostných testov.
9) V každom IT projekte sú určené a obsadené roly na strane Kancelárie NR SR, ktoré budú vykonávať správu a údržbu predmetu IT projektu po jeho zavedení do rutinnej prevádzky. Pokiaľ bude správu a údržbu vykonávať tretia strana, tak na strane Kancelárie NR SR je zriadená a obsadená rola vykonávajúca dohľad.
10) Pre každý nový informačný systém, alebo službu musia byť v návrhu a dokumentácii určené a dohodnuté kritériá pre jeho akceptáciu. Nový informačný systém musí byť testovaný podľa dohodnutých akceptačných kritérií skôr ako bude prijatý do prevádzky.
11) Súčasťou akceptačných kritérií musí byť aj preverenie implementácie dohodnutých bezpečnostných zásad a opatrení.
12) Pri definícií týchto rolí a ich následnom personálnom obsadzovaní musia byť určené a zohľadnené požiadavky na ich nezlučiteľnosť (nemožnosť kumulácie rolí v jednej osobe) a vzájomnú zastupiteľnosť.
13) Na zaistenie primeranej úrovne bezpečnosti musí byť v každom IT projekte vývojové a testovacie prostredie oddelené od produkčného prostredia.
14) Pri testovaní vyvíjaných komponentov sa štandardne nesmú použiť údaje z produkčného prostredia. Ak pre testovacie prostredie budú vytvorené analogické bezpečnostné opatrenia ako pre produkčné prostredie a charakter testov to vyžaduje, je akceptovateľné ich dočasné použitie iba pre výkon testov .
15) Pokiaľ výkon testov vyžaduje použitie osobných údajov, musia byť pred použitím anonymizované.
16) Ku každého IT projektu prevádzkovanému v prostredí Kancelárie NR SR musí jeho dodávateľ zabezpečiť vypracovanie a dodanie príslušnej projektovej dokumentácie pred zavedením IS do produkčnej prevádzky – používateľskej, administrátorskej a prevádzkovej dokumentácie k IS.
17) Používateľská dokumentácia je manuál na ovládanie IS používateľmi a existuje v takom rozsahu, aby používateľ vedel použiť všetky ponúkané funkcie, vrátane správneho použitia bezpečnostných mechanizmov.

18) Administrátorská dokumentácia je návod na správu a prevádzku IS.
19) Obsahom prevádzkovej dokumentácie je najmä popis architektúry, konfigurácií, integračných väzieb a rozhraní.
20) Všetky zmeny sú formálne riadené, schvaľované a zohľadňujú bezpečnostné požiadavky. Pre výkon zmien v IS sú stanovené pravidlá zabezpečujúce trvalé udržanie úrovne bezpečnosti IS.
21) Zamestnanci Kancelárie NR SR a pracovníci dodávateľov môžu zasahovať do konfigurácie prevádzkovaných IS iba v rozsahu svojej pôsobnosti, na základe plnenia pracovnej úlohy resp. v súlade s ustanoveniami zmluvy/SLA. Všetky vykonané zmeny sú vopred komunikované s vlastníkom dotknutého aktíva/aktív a zdokumentované.

Bezpečnosť v spolupráci s tretími stranami

1) Cieľom tejto oblasti bezpečnosti je zabezpečiť ochranu aktív Kancelárie NR SR, ku ktorým majú prístup dodávatelia a ďalšie tretie strany.
2) Pred začatím spolupráce a umožnením prístupu dodávateľov k aktívam Kancelárie NR SR musia byť vždy identifikované bezpečnostné požiadavky na túto spoluprácu a navrhnuté opatrenia minimalizujúce riziká vyplývajúce z tejto spolupráce. Tretia strana musí byť pred začatím spolupráce poučená o týchto požiadavkách, ktoré sú na ňu kladené zo strany Kancelárie NR SR, vrátane spôsobov identifikácie, nahlasovania a zvládania bezpečnostných incidentov.
3) Tretia strana, ktorá bude mať prístup k aktívam Kancelárie NR SR, bude pre Kanceláriu NR SR dodávať alebo poskytovať IT infraštruktúru, jej komponenty alebo súvisiace služby, musí mať s Kanceláriou NR SR uzatvorenú zmluvu alebo musí mať vzťah s Kanceláriou NR SR upravený iným relevantným právnym spôsobom, v závislosti od typu tretej strany a charakteru spolupráce.
4) Zodpovednosti za informačnú bezpečnosť v zmluvných vzťahoch s tretími stranami, servisnými a outsourcingovými partnermi sú explicitne vymedzené.
5) Tretia strana počas umožnenia prístupu k IS Kancelárie NR SR alebo údajom z IS Kancelárie NR SR, rešpektuje aplikovateľné ustanovenia bezpečnostnej politiky, interných dokumentov Kancelárie NR SR a relevantnej legislatívy.
6) Ak sa prevádzka časti IS alebo starostlivosť o niektoré aktíva IS prenáša na zmluvnú tretiu stranu (outsourcing), táto tretia strana má v zmluve vymedzenú zodpovednosť za ochranu aktív dotknutých outsourcingom. Tretia strana zabezpečuje výkon všetkých relevantných činností vyplývajúcich z bezpečnostnej politiky a súvisiacich predpisov.
7) V závislosti od charakteru služieb dodávaných treťou stranou sú zo strany Kancelárie NR SR priebežne monitorované a vyhodnocované s nimi súvisiace činnosti a parametre, najmä:
   a) využívanie vzdialených prístupov do siete Kancelárie NR SR,
   b) aktuálnosť prístupových oprávnení zamestnancov tretích strán,
   c) činnosti vykonávané na infraštruktúre a v aplikačnom vybavení,

d) úroveň dodržiavania SLA parametrov dodávaných služieb.

8) Zodpovednosť za riadenie vzťahu s treťou stranou je na strane Kancelárie NR SR priradená konkrétnemu zamestnancovi alebo organizačnému útvaru.

9) Zástupcovia zodpovedného organizačného útvaru sú pri uzatváraní zmluvy s treťou stranou na dodávku informačného systému, alebo služby povinní do zmluvy zabezpečiť zapracovanie povinnosti dodržiavať túto smernicu a ďalšie interné predpisy týkajúce sa informačnej bezpečnosti, ako aj záväzky vyplývajúce z práv ochrany duševného vlastníctva pre všetkých zamestnancov tretej strany, ktorí budú pracovať s informačnými aktívami kancelárie NR.

10) Pred poskytnutím akýchkoľvek informácií týkajúcich sa informačného systému kancelárie NR vrátane žiadosti o návrh riešenia musí byť s treťou stranou uzavretá dohoda o mlčanlivosti, ak nejde o výkon auditu podľa všeobecne záväzných právnych predpisov.

11) Bez dohody o mlčanlivosti nesmú byť poskytnuté tretej strane žiadne informácie týkajúce sa informačného systému úradu, požadovaných riešení, alebo služieb. Výnimku tvoria všeobecne známe skutočnosti a informácie, ktoré nie sú predmetom mlčanlivosti.

12) Pri nákupe informačného systému, alebo dodávke informačného systému a služieb od tretích strán musia byť bezpečnostné požiadavky a opatrenia určené v príslušnej dokumentácii už pri špecifikovaní technických požiadaviek.

13) Informačné systémy a služby dodávané tretími stranami musia spĺňať všetky zásady a opatrenia ustanovené internými predpismi úradu pre oblasť informačnej bezpečnosti.

14) Zamestnanci tretej strany, ktorý pracujú s informačnými aktívami kancelárie NR musia byť rovnako preukázateľne oboznámení s platnými bezpečnostnými zásadami a opatreniami. Záznam o tomto oboznámení zamestnancov musí byť súčasťou dokumentácie dodávaného informačného systému alebo služby.

15) Za oboznamovanie tretích strán a ich zamestnancov s internými predpismi týkajúcimi sa informačnej bezpečnosti je zodpovedný vlastník informačného aktíva. Spôsob a formu oboznámenia určí garant informačnej bezpečnosti.

16) Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať bezpečnostné zásady a opatrenia ustanovené v interných predpisoch a v dokumentácii navrhovaného diela.

17) Výnimku z bezpečnostných požiadaviek a opatrení môže v odôvodnených prípadoch na žiadosť zadávateľa udeliť garant informačnej bezpečnosti. V prípade rozporu o udelenie výnimky rozhoduje komisia pre riadenie informačnej bezpečnosti.

18) Výnimka z bezpečnostných požiadaviek a opatrení podľa článku 17 môže byť udelená výhradne na dobu pokiaľ trvajú dôvody, pre ktoré je požadovaná. Po uplynutí dôvodu musí byť výnimka bezodkladne zrušená.

19) Udelenie výnimky podľa odseku 17 musí mať písomnú formu a byť súčasťou dokumentácie dodávaného diela alebo služby a musí obsahovať najmä

    a. popis výnimky s odkazom na ustanovenie tejto smernice,
    b. dôvod, prečo je výnimka udelená,
    c. časové ohraničenie trvania výnimky,
    d. osobu zodpovednú za zrušenie výnimky po uplynutí dôvodu, pre ktorý bola udelená.

20) Zachovávanie bezpečnostných opatrení v informačných systémoch a službách dodaných tretími stranami musí byť priebežne monitorované a kontrolované tretími stranami ako aj úradom. Prípadné nedostatky musí tretia strana odstrániť v čo najkratšej dobe.
21) Ak sa identifikujú nové bezpečnostné riziká pri dodávke informačného systému tretími stranami, musia byť určené bezpečnostné opatrenia na ich elimináciu.
22) Bezpečnostné opatrenia informačných systémov a služieb dodaných tretími stranami musia byť prehodnotené aj v prípade ich významnej zmeny. V prípade vzniku bezpečnostného rizika pri zmene informačného systému, alebo služby musia byť treťou stranou dodatočne implementované bezpečnostné opatrenia eliminujúce zistené riziká.
23) Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia musí byť určená v zmluve s treťou stranou. Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia na ochranu osobných údajov úradu spravovaných treťou stranou (tzv. sprostredkovateľ) musí byť určená v zmluve s treťou stranou v samostatnej kapitole.

Príloha č. 1: Požiadavky na bezpečný návrh web aplikácií, návrh na základe metodík CSIRT SK

Požiadavky na bezpečný návrh web aplikácií

1. Webová stránka by mala pozostávať z verejných a privátnych zón a navigácia medzi nimi by nemala umožniť tok citlivých informácií medzi týmito zónami.
2. Citlivé informácie musia byť uchovávané v zašifrovanej podobe.
3. Validácia vstupov musí byť vykonávaná ako na strane klienta, tak aj na strane servera.
4. Produkčný a databázový server by mal byť umiestnený v zabezpečenej demilitarizovanej zóne (DMZ), ku ktorej môžu pristupovať len autorizované osoby.
5. Kód by mal byť udržiavaný, prehľadný a dokumentovaný.
6. Prezentačná vrstva musí byť oddelená od logickej vrstvy.

Šifrovanie

1. Na webový portál sa musí pristupovať prostredníctvom protokolu HTTPS.
2. Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu, na ktorej je dostupný webový portál.
3. Webový portál nesmie používať nedôveryhodné alebo exspirované SSL/TLS certifikáty.
4. Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.
5. Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.
6. Webový portál nesmie ukladať citlivé informácie v nezašifrovanej podobe na strane klienta, ani na strane servera.
7. Webový portál nesmie vkladať nešifrované zdroje bez SSL/TLS do stránok s SSL/TLS.

Šifrovacie kľúče a protokoly

1. Webový server nesmie podporovať protokoly SSLv2 a SSLv3.
2. Webový server musí podporovať TLS 1.2, pričom staršie verzie musia byť zakázané.
3. Webový server by mal podporovať TLS 1.3.
4. Webový server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.
5. Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku FREAK.
6. Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES).
7. Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku BREACH (Pri SSL/TLS musí byť vypnutá http kompresia).
8. Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku POODLE.
9. Použité šifry a protokoly SSL/TLS by mali byť odolné voči útoku LOGJAM.
10. Dĺžka kľúča asymetrickej šifry RSA, DSA v certifikáte by mala byť aspoň 2048 bitov.
11. Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).
12. Webový server by nemal podporovať RC4, DES a 3DES.
13. Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.
14. Konfiguráciu je možné otestovať v SSL teste od Qualys : https://www.ssllabs.com/ssltest/index.html.

Konfigurácia servera

1. Webový server nesmie podporovať klientom iniciovanú SSL/TLS renegociáciu šifrovacích kľúčov.

HTTP hlavičky a cookies

1. Server by mal pri SSL/TLS používať HSTS - HTTP Strict Transport Security.
2. V odpovediach webového servera sa nesmú nachádzať hlavičky prezrádzajúce použitú technológiu a / alebo jej verziu (Server, X-Powered-By, X-AspNet-Version a pod.)

3. V hlavičkách sa nesmú nachádzať informácie o použitých technológiách, backendových serveroch, internej infraštruktúre, ani bezpečnostných prvkoch.
4. Server musí používať hlavičku:
   a. X-Frame-Options : SAMEORIGIN // ochrana pred clickjackingom,
   b. X-XSS-Protection : 1 // čiastočná ochrana pred XSS.

Systém

1. Systém, nainštalované aplikácie a frameworky musia byť aktuálne z pohľadu bezpečnostných aktualizácií.
2. Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora.
3. Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.
4. Na serveri musia byť zatvorené všetky nepoužívané porty.

Webový server

1. Webový server by mal podporovať iba HTTP metódy POST a GET.
2. Webový server nesmie podporovať (musia byť vypnuté) HTTP metódy OPTIONS, TRACK a TRACE.
3. Webový server musí byť odolný voči SlowHTTP DoS (limitácia počtu spojení z jednej IP adresy, nastavenie timeoutu na HTTP requesty.)
4. Na webovom serveri musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy.
5. Ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté.
6. Webový server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia.
7. Webový server nesmie podporovať funkcionalitu listovania adresára (directory listing, Microsoft IIS tilde directory enumeration).
8. Súbor robots.txt alebo security.txt, resp. SECURITY, nesmie obsahovať odkazy na citlivé zdroje aplikácie (napríklad prihlasovanie administrátora a podobne).
9. Z webového servera musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.
10. Na webovom serveri by mal byť implementovaný WAF (web aplikačný firewall) minimálne s nasledujúcou funkcionalitou:
11. Detekcia a prevencia známych útokov (code injection – SQL, XSS, Command, XPATH),
12. Encoding a kontrola používateľských vstupov prostredníctvom whitelistingu.

Administrácia

1. Administračné rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).
2. Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.
3. Všetky servery a syslog servery musia byť synchronizované s NTP serverom, preferovaný je protokol PTP.
4. Administračné rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.

Aplikácia (webový portál)

1. Aplikácia musí ošetrovať všetky chyby a výnimky.
2. Aplikácia musí zobrazovať v prípade chyby aplikácie iba všeobecné chybové hlásenia.
3. V generovanom kóde nesmú byť prítomné komentáre, citlivé informácie a odkazy na vnútorné IP adresy.
4. Aplikácia musí pristupovať k ďalším aplikáciám a serverom prostredníctvom doménového mena (nie IP adresy, obzvlášť internej).
5. Aplikácia nesmie reflektovať obsahy hlavičiek v odpovedi servera.
6. Pre posielanie citlivých a autentifikačných údajov musí byť vynucované HTTPS spojenie.
7. Aplikácia nesmie ukladať citlivé údaje (napríklad session token) v URL adrese.
8. Aplikácia by nemala používať odkazy na externé zdroje (zdroje mimo správy).

9. Aplikácia nesmie používať odkazy na nedôveryhodné externé zdroje.
10. Všetky činnosti privilegovaných používateľov a administrátorov by mali byť zaznamenávané do log súborov prostredníctvom vzdialených logovacích serverov (syslog, Windows Event Forward).
11. Aplikácia nesmie používať funkciu eval().
12. Z aplikácie musia byť odstránené všetky ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov.

Autentizácia a autorizácia

1. Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).
2. Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu.
3. Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.
4. Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.
5. Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.
6. Aplikácia musí vyžadovať používanie silných hesiel (dĺžka aspoň 10 znakov, aspoň jedno veľké písmeno, malé písmeno, číslo a špeciálny znak).
7. Aplikácia musí vyžadovať pravidelnú zmenu hesla, musí byť nastavený minimálny a maximálny interval na zmenu hesla.
8. Aplikácia musí pri zmene hesla vyžadovať zadanie starého hesla.
9. Aplikácia musí po zmene hesla vyžadovať reautentizáciu.
10. Aplikácia by mala pri zmene hesla notifikovať používateľa zaslaním verifikačného emailu.
11. Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať salt.
12. Aplikácia musí implementovať funkcionalitu pre automatické odhlásenie po istej dobe nečinnosti.
13. Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.
14. Aplikácia musí podporovať simultánne paralelné prihlásenie iba z jednej verejnej IP adresy.
15. Aplikácia musí pri zmene verejnej IP adresy požadovať reautentifikáciu.
16. Aplikácia musí podporovať spustenie mechanizmu zamknutia účtu (lock-out) po istom počte neúspešných pokusov o prihlásenie (5)
17. Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie musí trvať aspoň 10 minút.
18. Zamknutie účtu po 5 neúspešných pokusoch o prihlásenie do kritického systému by malo trvať aspoň hodinu.
19. Je potrebné vytvárať log záznamy všetkých pokusov o autentizáciu (log-in, log-out, neúspešný log-in, žiadosť o zmenu hesla).
20. V prípade zamknutia účtu by aplikácia mala notifikovať zodpovednú osobu, resp. administrátora aplikácie.
21. Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať.
22. Aplikácia nesmie pre kritické systémy umožniť funkcionalitu zapamätania si hesla.

Používateľské vstupy

1. Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.
2. Aplikácia by mala používať parametrizované SQL požiadavky (queries).
3. Aplikácia nesmie využívať používateľské vstupy bez kontroly na tvorenie SQL dotazov.
4. Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SQL príkazoch (statements). Napríklad :
   - Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v názvoch súborov a zložiek.
   - Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v akomkoľvek skripte, databázovom dotaze alebo parametri príkazu operačného systému.
   - Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte HTML.
   - Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte JavaScript.

- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v kontexte REST API.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XML dokumentoch.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XPath požiadavkách (query). Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v XSL(T) style sheets.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v SSI príkazoch (statements).
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP hlavičkách.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v HTTP parametroch.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v LDAP požiadavkách.
- Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím v regulárnych výrazoch.

Relácie

1. Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.
2. Aplikácia nesmie povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.
3. Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.
4. Na generovanie CSRF tokenov musí aplikácia kryptograficky silný generátor pseudonáhodných čísel.
5. Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie.
6. Pri zmene prihlasovacích údajov (credentials) musí aplikácia znovu vygenerovať identifikátor relácie.
7. Pri zmene prihlasovacích údajov (credentials) musí aplikácia zneplatniť ostatné relácie.
8. Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.
9. Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.
10. Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.
11. Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).
12. Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.
13. Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.
14. Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.
15. Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia.
16. Relácia musí byť zviazaná s klientskou IP adresou.
17. Aplikácia musí vynucovať periodickú expiráciu a zneplatnenie relácií.

Nahrávanie súborov

1. Aplikácia musí nahrávané súbory ukladať mimo koreňového súboru pre dokumenty (document root), kde súčasne nesmie byť možnosť listovania adresára a nesmie byť možnosť interpretovať nahraté súbory ako napríklad skripty (PHP, ASP, JSP).
2. Aplikácia by nemala spúšťať a vyhodnocovať (evaluate) nahraté súbory.
3. Aplikácia musí vynucovať limit pre veľkosť nahratých súborov.
4. Aplikácia musí umožniť nahrávanie iba špecifických typov súborov a kontrolovať nielen ich príponu, ale aj MIME typ.
5. Aplikácia musí nahrávané súbory kontrolovať na prítomnosť škodlivého kódu prostredníctvom antimalware riešenia.

Obsah

1. Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.
2. Aplikácia by mala pre všetky poskytované stránky definovať „character set“.

Spracovanie XML

1. Aplikácia nesmie podporovať XML external entity expansion.
2. Aplikácia nesmie podporovať parsovanie XML external DTD.
3. Aplikácia nesmie podporovať všetky nadbytočné alebo nebezpečné XML rozšírenia.
4. Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

Rôzne

1. Aplikácia nesmie podporovať presmerovaniena používateľom poskytnuté externé umiestnenia.
2. Aplikácia musí obmedziť krížový prístup k doménam prostredníctvom whitelistingu.
3. Aplikácia musí pre všetky emailové funkcionality implementovať rate limiting.
4. Aplikácia musí pre všetky zdrojovo intenzívne funkcionality implementovať rate limiting.
5. Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

Príloha č. 2: Požiadavky na Bezpečnosť

Autentifikácia a autorizácia - minimálne požiadavky

1. Podpora technológií AD, LDAP, DB pre autentifikáciu a autorizáciu
2. Podpora protokolov Kerberos, SAML 2.0, TLS 1.2, RADIUS, PKI, Password-digest
3. Integrácia na Identity and Access Management napr AD
4. Možnosť zakázať preddefinované účty nevyžadujúce autentifikáciu (napr. Guest)
5. Možnosť zmeniť mená a heslá preddefinovaných účtov
6. Heslá alebo aj iné tajné zložky pre autentifikáciu majú byť chránené silnou kryptografiou pri ukladaní ako aj pri prenose
7. Chyba o prihlásení nesmie napovedať, ktorý prvok je nesprávny (meno, heslo, token, odpoveď)
8. Systém má podporovať okamžité zablokovanie používateľského konta, napríklad pri prekročení limitu neúspešných prihlásení.
9. Po úspešnom prihlásení má systém podporovať možnosť zobrazenia
   - času, dátumu a miesta posledného úspešného prihlásenia,
   - času a dátumu neúspešných pokusov o prihlásenie, ktoré predchádzali aktuálnemu úspešnému prihláseniu.
10. Informácie uvedené v bode 9 sú zaznamenávané prostredníctvom logovacieho nástroja
11. Možnosť integrácie s Citrix alebo možnosť použitia VPN (IPSec IKEv2) s klientskymi certifikátmi, či inou viac faktorovou autentifikáciou, v prípadoch prístupu cez nedôveryhodné siete.
12. Pred tým ako je používateľovi alebo inej entite umožnené vykonať požadovanú operáciu alebo pristúpiť k požadovaným dátam, musia byť úspešne ukončené kroky autentizácie a autorizácie v uvedenom poradí.
13. Systém alebo aplikácia musí mať vhodný riadiaci mechanizmus na autentifikáciu a autorizáciu, aby sa dal vhodne nastaviť prístupový profil.
14. Propagácia identity používateľa cez všetky vrstvy (FE, ML, BE) nepopierateľným spôsobom (HMAC, digitálny podpis)
15. Propagácia jednoznačného identifikátora flow_ID (unikátny pre každý request používateľa) cez všetky vrstvy (FE, ML, BE) nepopierateľným spôsobom (HMAC, digitály podpis)
16. Systém musí umožniť RBAC (riadenie prístupu na základe rolí).
17. Komponenty (aplikácia, služby) bežia alebo sa autentifikujú pod používateľom/účtom s minimálnymi oprávneniami, teda len takými, ktoré sú potrebné pre plnenie ich funkcie. Napr. aplikácia v režime normálneho používania nepotrebuje prístup na databázu db_owner.
18. Opätovná autorizácia sa musí vyžadovať pred každou individuálnou operáciou, pričom je možné použiť caching oprávnení.
19. Opätovná autorizácia a autentifikácia sa musí vyžadovať po vypršaní vymedzenej doby.
20. Aplikácie, služby a databáza majú byť navrhnuté, štruktúrované a implementované tak, aby mohli byť vytvorené používateľské prístupové profily umožňujúce odlíšenie a oddelenie operácií (read, insert, delete, edit) a rôzne stupne klasifikácie (Prísne citlivé a citlivé a ostatné)
21. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
   - V2: Authentication Verification Requirements
   - V3: Session Management Verification Requirements
   - V4: Access Control Verification Requirements
   aktuálnej verzie štandardu OWASP Application Security Verification
   URL:
   https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads

Monitorovanie, logovanie a auditovanie - minimálne požiadavky

1. Aplikácie, služby a systémy majú mať zdokumentovaný zoznam udalostí, ktoré sú auditované.
2. Pre aplikácie, služby a systémy sú v logoch zaznamenávané minimálne nasledovné udalosti:
   - spustenie a vypnutie
   - nekorektné ukončenie činnosti
   - úspešné a neúspešné prihlásenie a prístup
   - spustenie a vypnutie funkcií logovania
   - spustenie a zastavenie súčastí
   - vymazanie a modifikácia programových a konfiguračných súborov
3. O udalostiach sa zaznamenávajú minimálne nasledovné údaje:
   - meno a jednoznačný identifikátor udalosti
   - dátum a čas začiatku (a konca) udalosti
   - jednoznačný identifikátor a meno pre zdrojový systém/aplikáciu/službu
   - jednoznačný identifikátor účtu používateľa, pod ktorým udalosť nastala
4. Zaznamenávanie chýb súvisiacich s neočakávaným alebo nesprávnym vstupom (napr. neočakávaný vstup z dropdown listu, nesprávny formát vstupného reťazca).
5. Prístupové oprávnenia nad súbormi logov sú reštriktívne tak, aby do nich mohol do nich zapisovať len vlastniaci komponent (aplikácia, systém, služba), a aby mohli byť čítané len administrátorom komponentu, či na to určeným komponentom pre účely centralizovaného zberu logov a udalostí.
6. Integrita log a audit záznamov musí byť chránená (napr. HMAC alebo PKI digitálnym podpisom)
7. Podpora štandardných formátov exportu log súborov.
8. Podpora Syslog
9. Čas všetkých systémov musí byť zosynchronizovaný podľa rovnakého zdroja času spoločnosti tak, aby boli logy a audit záznamy zarovnané podľa jedného zdroja času.
10. Riešenie má byť integrované so SIEM na systémovej ako aj aplikačnej a databázovej vrstve.
11. Žiadna Exception či chyba nesmie byť neošetrená
12. Žiadna Exception či informácia o chybe nesmie doraziť na end-usera. Na end-usera môže doraziť len generická hláška o chybe bez detailov a informácií o jej povahe
13. Systémové, aplikačné a databázové logy majú byť centrálne zbierané v dostatočne krátkych intervaloch (online, alebo max do 1h) a uchovávané týmto riešením a na to dedikovaným systémom, alebo na to určeným systémom.
14. Všetky log súbory majú byť pomenované a klasifikované s určením retenčnej periódy pre lokálne a centrálne úložiská.
15. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
    - V8. Error handling and logging
    aktuálnej verzie štandardu OWASP Application Security Verification
    URL:
    https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads

Architektúra, Infraštruktúra a Platforma - minimálne požiadavky

1. Je požadovaná viacvrstvová architektúra definujúca FE, ML a BE vrstvy, ako aj dátové a manažment toky, ktorá je oddelená:
   a. Sieť: VLAN, avšak kritické a prísne citlivé systémy je potrebné oddeliť fyzicky LAN
   b. Klient – Server architektúra: citlivé by mali byť oddelené FE a ML (Mandatory) minimálne na úrovni vizualizácie (iný guest v rámci HV), avšak BE má byť dodelený minimálne na úrovni HV (iný HV - Hypervisor) , oddelenie prísne citlivé od ostaných na úrovni HV a oddeliť aj FE, ML aj BE na úrovni HV. Toto má byť zohľadnené všetkými firewallmi."
2. Spracovávanie a ukladanie dát pre rôzne agendy má byť oddelené minimálne na logickej úrovni (pre citlivé) a na virtualizačnej úrovni (prísne citlivé) cez všetky vrstvy

3. Všetky aplikácie, služby, systémy, servery, sieťové prvky sú zabezpečené v zmysle hardeningu v súlade s relevantnými best practices a medzinárodnými štandardmi.
4. Webové aplikácie a služby sú publikované len cez web aplikačný firewall.
5. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
   - V1. Architecture, design and threat modelling
   - V15. Business logic
   - V19. Configuration
   aktuálnej verzie štandardu OWASP Application Security Verification
   URL:
   https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads
6. Každý prenos prísne citlivých dát je chránený TLS 1.2 (SSH, VPN) protokolom so vzájomnou autentifikáciou (použitím X.509) a na aplikačnej vrstve podpisom a šifrovaním silnou kryptografiou. Veľký objem citlivých dát sa považuje za prísne citlivý (súbor).
7. Zvlášť citlivé dáta sú chránené pri ukladaní podpisom a šifrovaním silnou kryptografiou
8. Citlivé a dáta sa chránia pri prenose cez nedôveryhodné siete šifrovaním silnou kryptografiou, TLS 1.2 protokolom alebo SSH.
9. Každé spojenie musí byť autentifikované použitím silnej kryptografie, v opačnom prípade nie je spojenie akceptované.
10. Všetky manažment a autentifikačné toky musia byť šifrované.
11. Na vrstve správ (message level) sa môže používať len SOAP web servisy, ktoré sú chránené šifrovaním a digitálnym podpisom silnou kryptografiou. V prípade, že je nutné použiť iný typ správ (napr. JSON), je nutné popísať spôsob zaistenia bezpečnosti na úrovni správ.
12. "Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
    - V9. Data protection
    - V10. Communications
    - V11. HTTP security configuration
    - V18. Web services
    aktuálnej verzie štandardu OWASP Application Security Verification
    URL:
    https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads"

Integrita systému, aplikácie, služieb a dát - minimálne požiadavky

1. Má byť zaistená integrita systémov a aplikácií a služieb tak, že sa kontroluje ich integrita pri spúšťaní automatizovane (digitálny podpis).
2. Systém má byť chránený antilmalware riešením, ak je to možné
3. Systém musí byť chránený firewallom, a ak možné, tak aj host intrusion prevention systémom.
4. Aplikácia a služba musí validovať správnosť a platnosť dát na vstupe pred začatím ich spracovávania.
5. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
   - V5. Malicious input handling
   - V13. Malicious controls
   - V16. File and resources
   aktuálnej verzie štandardu OWASP Application Security Verification
   URL:

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads

Kryptografia - minimálne požiadavky

1. Privátne kľúče, symetrické kľúče, heslá, odpovede sú ukladané šifrovane a je zabezpečená minimalizácia rizika ich neoprávneného použitia, podľa vhodnosti je použitý HSM.
2. Povolené kryptografické algoritmy majú byť založené na minimálne AES 256 GCM (XTS), SHA 256, RSA 2048, Diffie-Hellman 2018, ECDSA 163
3. TLS 1.2
4. Password-digest (SHA-256, NONCE 256bit)
5. IPSec, IKEv2
6. WS-Security Policy 1.2
7. RADIUS CHAP alebo EAP (len silné metódy), TACACS+
8. Kerberos
9. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
   - V7. Cryptography at rest
   aktuálnej verzie štandardu OWASP Application Security Verification
   URL:
   https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads"

Mobilné aplikácie - minimálne požiadavky

1. Uplatňujúc level (3 - pre prísne citlivé, 2 - citlivé, 2 - verejné, 1 - interné) vyhovieť relevantným požiadavkám a vypracovať stručnú dokumentáciu (odpoveď a spôsob naplnenia požiadavky s prípadnou referenciou na dokumentáciu) podľa častí:
   - V17. Mobile
   aktuálnej verzie štandardu OWASP Application Security Verification
   URL:
   https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project#tab=Downloads

Business Continuity - minimálne požiadavky

1. V prípade zaplnenia kapacity pre auditné záznamy, systém túto skutočnosť musí alertovať kompetentným osobám dostatočne včas, aby sa zamedzilo možnej strate informácií či nesprávnemu fungovaniu systému.
2. Systém musí umožniť spustenie definovaných selftestov počas štartu systému a manuálne (kontrola dostupnosti komponentov, integrita).
3. Aplikácia, služby, systémy a servery musia mať stanovené jasné požiadavky špecifikujúce, ktoré objekty a dáta musia byť zálohované, ako často musia byť zálohované, ako dlho majú a môžu byť zálohované, ako majú byť uschované a ako spracovávané za účelom zabezpečenia súladu s biznis požiadavkami a požiadavkami legislatívy a štandardmi.
4. Riešenie má poskytovať fault tolerance, high availability a disaster recovery.
5. Možnosť efektívneho a štandardného exportovania a importovania dát, aplikácie a systémov so zabezpečením dátovej integrity.

Penetračné testovanie a bezpečnostný audit - minimálne požiadavky

1. Súčinnosť pri výkone penetračného testu v zmysle balckbox a graybox
2. Nálezy z penetračného testovania stupňa critical, high a medium majú byť ihneď odstránené a ich odstránenie je podmienkou nasadenia riešenia do produkčnej prevádzky

Business Continuity - minimálne požiadavky

1. RACI matica
2. Bezpečnostná architektúra riešenia popisujúca minimálne:
   - architektúru riešenia
   - dátové, autentifikačné a manažment toky
   - komunikačné protokoly pre vrstvy 4, 5, 6, 7 ISO/OSI, aj s portmi a smermi
   - zóny a vrstvy (public, extranet, intranet, FE ML, BE)
   - autentifikáciu a autorizáciu
   - kryptografický manažment
   - aplikačnú bezpečnosť
   - šírenie identity a identifikátora requestov (flow_ID)
   - architektúru vysokej dostupnosti
   - architektúru zálohovania a obnovy zo zálohy v zmysle disaster recovery
   - integráciu s relevantnými bezpečnostnými funkciami
   - architektúru cez všetky relevantné prostredia (ako napr. Dev, T, OSA, PROD)
3. Štandardná bezpečnostná dokumentácia pre projekty:
   - Inventár informačných aktív s ich klasifikáciou a kategorizáciou
   - RA: Analýza rizík s cost benefit analýzou
   - RA: Správa z analýzy rizík
   - SCL: Zoznam bezpečnostných opatrení
   - SQAP: Plán zaistenia bezpečnosti
   - STSA: Rozsah a metódy testovania
   - STTS: Scenáre a požiadavky pre bezpečnostné testovanie
   - Plán odstránenia zistených nedostatkov
   - Vyplnený APP_Dotazník
   - Záverečný report z bezpečnostného testovania
   - Návod na obsluhu, administráciu, konfiguráciu, inštaláciu a nasadzovanie
   - Disaster recovery procedúru s reportom z DR testu
   - SLA
   - OLA
   - Návrh (zmeny - ak aplikovateľné) vnútorného predpisu pre bezpečnú prevádzku, údržbu a zmenu riešenia vrátane riadenia identít a prístupov