Zmluva
o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností
uzatvorená podľa § 269 ods. 2 zákona č. 513/1991 Zb. Obchodný zákonník v znení neskorších predpisov a § 19 ods. 2 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Čl. I
Zmluvné strany

Prevádzkovateľ

Obchodné meno:	**Slovenská záručná a rozvojová banka, a. s.**
Sídlo:	Štefánikova 27, Bratislava – mestská časť Staré Mesto 811 05
Zápis:	v obchodnom registri vedenom Mestským súdom Bratislava III, oddiel Sa, vložka č. 3010/B,
Štatutárny orgán:	Ing. Radko Kuruc, PhD., predseda predstavenstva Ing. Pavel Mockovčiak, člen predstavenstva
IČO:	00 682 420
DIČ:	2020804478

(ďalej aj ako „**prevádzkovateľ**“ alebo „**SZRB**“ alebo „**objednávateľ**“)
a

Dodávateľ

Obchodné meno:	**Aricoma Systems s.r.o.**
Sídlo:	Krasovského 14 Bratislava - mestská časť Petržalka 851 01
Zápis:	v obchodnom registri vedenom Mestským súdom Bratislava III, oddiel Sro, vložka č. 130357/B
Štatutárny orgán:	Mario Háronik, konateľ
IČO:	36 396 222
DIČ:	2020105428
IČ pre DPH:	SK2020105428
Bankové spojenie:	
IBAN:	

(ďalej aj ako „**dodávateľ**“ alebo „**poskytovateľ**“)

(spolu ďalej ako „**zmluvné strany**“)

Čl. II
Preambula

1. Prevádzkovateľ je podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**zákon o kybernetickej bezpečnosti**“) prevádzkovateľom základnej služby podľa § 3 zákona o kybernetickej bezpečnosti. Dodávateľ je podľa § 19 ods. 2 zákona o kybernetickej bezpečnosti treťou stranou, ktorá na základe zmluvy na výkon činností poskytuje prevádzkovateľovi činnosti, ktoré priamo súvisia

s prevádzkou sietí a informačných systémov pre prevádzkovateľa, ako prevádzkovateľa základnej služby.

2. Zmluvné strany uzatvárajú za účelom špecifikácie plnenia bezpečnostných opatrení a notifikačných povinností v súlade s § 19 ods. 2 zákona o kybernetickej bezpečnosti a podľa § 9 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „**Vyhláška č. 362/2018**“) túto Zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ďalej len „**Zmluva**“).

3. Zmluvné strany uzatvárajú túto Zmluvu v súvislosti s poskytovaním služieb dodávateľom ako poskytovateľom služieb v prospech objednávateľa (ktorý je prevádzkovateľom) týkajúcich sa užívania počítačového programu s názvom systém IDM AC Identita Prevádzkovateľom na základe osobitnej Zmluvy o poskytovaní služieb uzatvorenej dňa (ďalej len „**Zmluva na výkon činností**“).

Čl. III
Predmet zmluvy

1. Predmetom tejto Zmluvy je stanovenie základných úloh a princípov spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť pri prevádzke sietí a informačných systémov prevádzkovateľa počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom (ďalej len „**kybernetický incident**“), ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa a minimalizovať vplyv kybernetických incidentov na kontinuitu prevádzkovania sietí a informačných systémov prevádzkovateľa, s prevádzkou ktorých priamo súvisí výkon činností dodávateľa na základe Zmluvy na výkon činností.

Čl. IV
Práva a povinnosti zmluvných strán

1. Dodávateľ sa zaväzuje:

a. dodať zoznam svojich pracovníkov a ich pracovných rolí , ktoré majú mať prístup k informáciám a údajom prevádzkovateľa, s povinnosťou oznámiť prevádzkovateľovi každú zmenu v personálnom obsadení; dodávateľ zabezpečí, že pracovníci dodávateľa zúčastnení na poskytovaní služieb v zmysle Zmluvy o výkone činností podpíšu vyjadrenie o zachovávaní mlčanlivosti podľa zákona o kybernetickej bezpečnosti,
b. umožniť vykonanie kontrolných činností a auditu prevádzkovateľom u dodávateľa,
c. ustanoviť spôsob a formu hlásenia ďalších informácií požadovaných prevádzkovateľom na plnenie povinností prevádzkovateľa vyplývajúcich zo zákona o kybernetickej bezpečnosti a ich vymedzenie,
d. dodržiavať Štandard kybernetickej bezpečnosti v Slovenskej záručnej a rozvojovej banke, a. s., ktorého znenie tvorí príloha č. 1 tejto Zmluvy.

2. Dodávateľ je povinný plniť notifikačné povinnosti na úseku kybernetickej bezpečnosti v rozsahu uvedenom v tejto Zmluve.

3. Dodávateľ je povinný chrániť všetky informácie ku ktorým má prístup na základe Zmluvy na výkon činností alebo tejto Zmluvy, alebo ktoré mu boli poskytnuté zo strany prevádzkovateľa s tým, že všetci dotknutí zamestnanci dodávateľa jeho subdodávatelia a/alebo iné tretie osoby, prostredníctvom ktorých dodávateľ poskytuje služby podľa Zmluvy na výkon činností (ďalej len „**tretia osoba**“ alebo „**subdodávateľ**“) sú povinní podpísať vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 zákona o kybernetickej bezpečnosti.

4. Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto Zmluvy v bezpečnostnej dokumentácii, ktorá je aktuálna a musí zodpovedať aktuálnemu stavu. Bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi.

5. Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia na účely plnenia tejto Zmluvy minimálne v oblastiach podľa § 20 ods. 3 písm. d), g) až i), k) a m) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, § 11, § 12, § 13, § 15 a § 17 Vyhlášky č. 362/2018 a v rozsahu špecifikovanom v bezpečnostných politikách prevádzkovateľa.
6. Dodávateľ je povinný doručiť prevádzkovateľovi zoznam zamestnancov dodávateľa subdodávateľa a tretích osôb ako aj ich pracovných rolí, ktorí sa budú podieľať na plnení činností podľa Zmluvy na výkon činností a tejto Zmluvy a ktorí budú mať prístup k informáciám prevádzkovateľa (ďalej len „**zoznam osôb**"). Dodávateľ je povinný oznámiť prevádzkovateľovi každú zmenu v zozname zamestnancov podľa tohto bodu a to elektronicky prostredníctvom elektronickej správy (emaily uvedené v čl. XI tejto zmluvy). Dodávateľ je povinný zabezpečiť, aby každá osoba uvedená v zozname osôb, schválená odborom bezpečnosti informačných technológií prevádzkovateľa a riaditeľom odboru informačných systémov prevádzkovateľa podpísala vyhlásenie o mlčanlivosti a zúčastnila sa na vstupnom poučení o ochrane osobných údajov pred nástupom na výkon zmluvných činností na základe Zmluvy na výkon činností. Po podpísaní vyhlásenia o mlčanlivosti budú týmto osobám sprístupnené bezpečnostné politiky prevádzkovateľa.
7. Dodávateľ je povinný písomne informovať prevádzkovateľa o každej zmene, ktorá má významný vplyv na bezpečnostné opatrenia realizované dodávateľom na účely plnenia tejto Zmluvy.
8. Prevádzkovateľ je povinný informovať v nevyhnutnom rozsahu dodávateľa o hlásenom kybernetickom incidente za predpokladu, že by sa najmä plnenie zo Zmluvy o výkone činností stalo nemožným. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.
9. Dodávateľ môže za účelom plnenia svojho záväzku podľa Zmluvy na výkon činností ustanoviť ďalšieho dodávateľa , ktorý bude úplne alebo čiastočne zabezpečovať plnenie pre prevádzkovateľa namiesto pôvodného dodávateľa, avšak za splnenia nasledovných podmienok:
   a) dodávateľ môže ustanoviť subdodávateľa iba na základe predchádzajúceho písomného súhlasu prevádzkovateľa; dodávateľ v žiadosti o udelenie súhlasu písomne oznámi prevádzkovateľovi obchodné meno a ostatné identifikačné údaje subdodávateľa,
   b) dodávateľ je povinný zmluvne zaviazať subdodávateľa k plneniu povinnosti podľa Zmluvy na výkon činností a tejto Zmluvy, a uložiť mu rovnaké povinnosti týkajúce sa plnenia bezpečnostných opatrení a notifikačných povinnosti za účelom zabezpečenia kybernetickej bezpečnosti sieti a informačných systémov prevádzkovateľa, ako sú ustanovené v tejto Zmluve, uložiť mu povinnosť poskytnutia dostatočných záruk na vykonanie primeraných technických opatrení takým spôsobom, aby spracúvanie spĺňalo požiadavky najmä NARIADENIA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „nariadenie GDPR") a ďalšie povinnosti dojednane s prevádzkovateľom v osobitnej zmluve týkajúcej sa ochrany osobných údajov,
   c) zodpovednosť voči prevádzkovateľovi nesie dodávateľ, ak subdodávateľ nesplní svoje povinnosti tykajúce sa Zmluvy na výkon činností a tejto Zmluvy, tým nie je dotknutý nárok Dodávateľa na náhradu škody voči subdodávateľovi.

Čl. V
Okolnosti plnenia Zmluvy

1. Pojmy používané v tejto Zmluve majú význam v zmysle zákona o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.
2. Dodávateľ vyhlasuje, že sa detailne oboznámil s rozsahom a povahou požadovaných bezpečnostných opatrení a notifikačných povinností podľa tejto Zmluvy a že disponuje potrebným technickým, technologickým a personálnym vybavením, kapacitami a odbornými znalosťami, ktoré sú potrebné na plnenie úloh vyplývajúcich zo zákona o kybernetickej bezpečnosti a z tejto Zmluvy, a že má zavedené úlohy, procesy, role a technológie v organizačnej personálnej a technickej oblasti, ktoré sú potrebné na napĺňanie požiadaviek zákona o kybernetickej bezpečnosti a tejto Zmluvy.

3. Plnenie povinností podľa tejto Zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa podľa Zmluvy na výkon činností. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto Zmluvy počas celej doby trvania Zmluvy na výkon činností.
4. Odplata za plnenie povinností dodávateľa podľa tejto Zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto Zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom dodávateľovi podľa Zmluvy na výkon činností a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto Zmluvy nemá nárok.

Čl. VI
Bezpečnostné opatrenia na predchádzanie kybernetickým incidentom

Dodávateľ je povinný v rámci prevencie kybernetických incidentov, ktoré by mohli mať nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa, a tým na činnosť prevádzkovateľa:

a. zabezpečiť vlastnú kybernetickú bezpečnosť, aby pri poskytovaní elektronických komunikačných služieb a sietí cez siete a informačné systémy dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa,
b. vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení Zmluvy na výkon činností a tejto Zmluvy alebo budú mať prístup k informáciám prevádzkovateľa,
c. sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov kybernetických incidentov všeobecne,
d. sledovať hrozby týkajúce sa dodávateľa, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
e. predchádzať hrozbe vzniku kybernetických incidentov,
f. v prípade vzniku kybernetických incidentov, systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o kybernetických incidentoch,
g. prijímať od prevádzkovateľa varovania pred kybernetickými incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potencionálny nepriaznivý vplyv na siete a informačné systémy prevádzkovateľa,
h. zasielať prevádzkovateľovi včasné varovania pred kybernetickými incidentmi, o ktorých sa dozvie z vlastnej činnosti podľa tejto Zmluvy alebo inak, a
i. spolupracovať s prevádzkovateľom pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa.

Čl. VII
Riešenie kybernetických incidentov

1. Dodávateľ je povinný bezodkladne hlásiť každý kybernetický incident prevádzkovateľovi, ktorý by mohol mať vplyv na bezpečnosť dát prevádzkovateľa spôsobom určeným prevádzkovateľom, ktorý je uvedený v bezpečnostnej politike, vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie kybernetických incidentov. Ak od okamihu hlásenia kybernetického incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie kybernetického incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.
2. Dodávateľ je povinný riešiť kybernetický incident najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení kybernetického incidentu na mieste, reakciou na kybernetický incident a podporou reakcií na kybernetický incident.
3. Pri riešení kybernetických incidentov je dodávateľ povinný na žiadosť prevádzkovateľa spolupracovať s prevádzkovateľom, Národným bezpečnostným úradom SR, orgánom činným v trestnom konaní a príslušným Ministerstvom (ďalej len „**príslušný orgán**“), na tento účel

im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto Zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie kybernetického incidentu.

4. Dodávateľ je povinný oznámiť prevádzkovateľovi skutočnosti, či v súvislosti s kybernetickým incidentom mohlo dôjsť k spáchaniu trestného činu.
5. Dodávateľ je povinný v čase kybernetického incidentu zabezpečiť dôkazný prostriedok tak, aby mohol byť použitý v prípadnom trestnom konaní a poskytnúť ho prevádzkovateľovi.
6. Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi vykonanie opatrenia na riešenie kybernetického incidentu a jeho výsledok.
7. Po vyriešení kybernetického incidentu je dodávateľ na výzvu prevádzkovateľa v určenej lehote povinný predložiť prevádzkovateľovi návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu kybernetického incidentu (ďalej len „**ochranné opatrenie**“) na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote alebo, ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom na návrhu nového ochranného opatrenia.
8. Po schválení ochranného opatrenia prevádzkovateľom je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať, po jeho vykonaní preveriť jeho účinnosť a výsledok oznámiť prevádzkovateľovi.
9. Dodávateľ je povinný informovať prevádzkovateľa aj o akýchkoľvek iných skutočnostiach, ktoré môžu mať vplyv na zabezpečenie kybernetickej bezpečnosti, a to elektronicky prostredníctvom elektronickej správy .

Čl. VIII
Mlčanlivosť

1. Dodávateľ je povinný zachovávať mlčanlivosť o všetkých skutočnostiach, o ktorých sa dozvie v súvislosti s plnením Zmluvy na výkon činností a tejto Zmluvy a ktoré nie sú verejne známe, pokiaľ by sa mohli dotýkať oblasti kybernetickej bezpečnosti. V prípade pochybností platí, že skutočnosť sa dotýka kybernetickej bezpečnosti. Dodávateľ je najmä povinný chrániť informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí.
2. Povinnosť zachovávať mlčanlivosť trvá aj po skončení tejto Zmluvy, pričom výnimky z povinnosti mlčanlivosti upravuje zákon o kybernetickej bezpečnosti.
3. Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti aj jeho zamestnanci, subdodávatelia a ich zamestnanci, ako aj prípadná tretia osoba a to aj po zániku ich pracovnoprávneho alebo obdobného vzťahu.
4. Dodávateľ je povinný hlásiť prevádzkovateľovi za účelom plnenia povinnosti prevádzkovateľa vyplývajúcich zo Zákona o kybernetickej bezpečnosti všetky ďalšie prevádzkovateľom požadované informácie, najmä informácie potrebné pre:
    a) riešenie kybernetického incidentu,
    b) hlásenie závažného kybernetického incidentu,
    c) poskytnutie súčinnosti a spolupráce s Národným bezpečnostným úradom SR,
    d) zabezpečenie dôkazu alebo dôkazného prostriedku tak, aby mohol byť použitý v trestnom konaní,
    e) oznámenie orgánu činnému v trestnom konaní, že bol spáchaný trestný čin, ktorého sa kybernetický incident týka.
5. Dodávateľ je povinný realizovať hlásenia podľa ods. 4. tohto článku Zmluvy a komunikovať s prevádzkovateľom pri plnení povinnosti podľa tejto Zmluvy spôsobom a formou určeným prevádzkovateľom v článku XI. tejto Zmluvy.

Čl. IX
Audit kybernetickej bezpečnosti

1. Prevádzkovateľ je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto Zmluvy a efektívnosti ich plnenia, najmä na overenie

technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh na úseku kybernetickej bezpečnosti, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov na základe zákona o kybernetickej bezpečnosti a tejto Zmluvy.

2. Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, ak v Zmluve o výkone činností nie je dohodnuté niečo iné.
3. Prevádzkovateľ môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby, v takom prípade práva a povinnosti prevádzkovateľa pri výkone auditu realizuje prevádzkovateľom poverená tretia osoba.
4. Dodávateľ je pri audite povinný spolupracovať s prevádzkovateľom a sprístupniť mu svoje priestory, dokumentáciu, technické a technologické vybavenie, ktoré súvisí s plnením úloh na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
5. Prevádzkovateľ je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh a úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
6. V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi súlad s touto Zmluvou, najmä preukázať svoju pripravenosť plniť úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov a alebo tretiu osobu o povinnosti mlčanlivosti podľa tejto Zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.
7. Prevádzkovateľ je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer vykonať u dodávateľa audit.
8. Vykonanie alebo nevykonanie auditu prevádzkovateľom nezbavuje zodpovednosti dodávateľa za plnenie jeho povinností vyplývajúcich z tejto Zmluvy.
9. Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy na úseku kybernetickej bezpečnosti podľa tejto Zmluvy.
10. Prevádzkovateľ je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe.

Čl. X
Osobitné ustanovenia

1. Dodávateľ je povinný plniť povinnosti podľa tejto Zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi, vrátane všeobecných bezpečnostných opatrení, sektorových bezpečnostných opatrení, ak boli vydané príslušným orgánom, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým incidentom a zásadami riešenie kybernetických incidentov, ktoré vydáva Národný bezpečnostný úrad SR v oblasti kybernetickej bezpečnosti.
2. Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa alebo by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa a prevádzky elektronických komunikačných služieb alebo sietí tak, aby nebola narušená ich dostupnosť, dôvernosť, autentickosť a integrita.
3. Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto Zmluvy (vrátane evidovania kybernetických incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa mu predložiť uvedenú dokumentáciu.
4. Dodávateľ je povinný plniť povinnosti podľa tejto Zmluvy odo dňa jej účinnosti.
5. V prípade, ak dodávateľ plní Zmluvu na výkon činností prostredníctvom svojich subdodávateľov a toto plnenie priamo súvisí s poskytovaním elektronických komunikačných služieb alebo sietí v súvislosti s prevádzkou sietí a informačných systémov prevádzkovateľa, je povinný zabezpečiť plnenie povinností na úseku kybernetickej bezpečnosti vyplývajúcich z tejto Zmluvy aj u svojich subdodávateľov tak, aby boli naplnené ciele tejto Zmluvy. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ mohol vykonať audit v súlade s touto Zmluvou aj u týchto subdodávateľov.
6. Všetky informácie, ktoré majú vplyv na plnenie práv a povinností uvedených v tejto Zmluve sú zmluvné strany povinné si bezodkladne navzájom oznámiť, a to písomne na adresy

uvedené v záhlaví tejto Zmluvy, a zároveň elektronicky prostredníctvom elektronickej správy (emaily uvedené v Čl. XI tejto zmluvy).

7. Dodávateľ vyhlasuje, že si je vedomý, že neplnenie jeho povinností vyplývajúcich z tejto Zmluvy by ohrozilo plnenie účelu tejto Zmluvy, čím by bola ohrozená kybernetická bezpečnosť prevádzkovateľa. Vzhľadom na uvedenú skutočnosť, dodávateľ zodpovedá za porušenie akýkoľvek záväzkov vyplývajúcich mu z tejto Zmluvy, zákona o kybernetickej bezpečnosti alebo Vyhlášky č. 362/2018 a za dôsledky a škodu vzniknutú v dôsledku kybernetických incidentov, ktoré by sa pri riadnom a včasnom plnení povinnosti podľa tejto Zmluvy neprejavili alebo by sa prejavili v menšej intenzite a rozsahu, v celom rozsahu. Prevádzkovateľ má nárok na preukázanú náhradu škody, pokuty alebo iné náklady, ktoré prevádzkovateľovi vzniknú v súvislosti s porušením uvedených záväzkov dodávateľa.
8. Po ukončení tejto Zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa všetky informácie, ku ktorým mal počas trvania tejto Zmluvy prístup, resp. podľa pokynu prevádzkovateľa tieto informácie zničiť, ak osobitný predpis alebo medzinárodná zmluva, ktorou je Slovenská republika viazaná, nepožaduje uchovávanie týchto informácií na strane dodávateľa. To zahŕňa predovšetkým, ale nielen, systémové špecifikácie, prístupové informácie, zálohy a ďalšie technologické špecifikácie o informačných systémoch a sieťach prevádzkovateľa.

Čl. XI
Kontaktné osoby pre kybernetickú bezpečnosť

1. Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto Zmluvy s prevádzkovateľom spôsobom určeným prevádzkovateľom, a to elektronicky prostredníctvom elektronickej správy (email -), pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.
2. Kontaktná osoba prevádzkovateľa pre komunikáciu s dodávateľom na úseku kybernetickej bezpečnosti je: Ing. Roman Šebo, riaditeľ odboru bezpečnosti informačných technológií, .
3. Kontaktná osoba dodávateľa pre komunikáciu s prevádzkovateľom na úseku kybernetickej bezpečnosti je: .
4. Kontakt na zástupcu prevádzkovateľa na úseku kybernetickej bezpečnosti je: .
5. Kontakt na zástupcu dodávateľa na úseku kybernetickej bezpečnosti je: .
6. Kontaktné osoby podľa bodov 2. až 5. tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme na adresu zmluvnej strany uvedenú v záhlaví tejto Zmluvy alebo elektronicky prostredníctvom elektronickej správy – kontakt na prevádzkovateľa: a kontakt na dodávateľa: .

Čl. XII
Záverečné ustanovenia

1. Táto Zmluva podlieha povinnému zverejneniu podľa § 5a ods. 1 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (zákon o slobode informácií) a v súlade s § 47a zákona č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov.
   Táto Zmluva nadobúda platnosť dňom jej podpísania oprávnenými zástupcami oboch zmluvných strán. Táto Zmluva nadobúda účinnosť dňom **01.05.2024** po splnení nasledovných odkladacích podmienok:
   a) táto Zmluva bude zverejnená v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky **najneskôr ku dňu 30.04.2024**,
   b) nadobudne účinnosť Zmluva na výkon činností. Zmluvné strany sa ďalej dohodli, že zverejnenie tejto Zmluvy zabezpečí prevádzkovateľ najneskôr **ku dňu 30.04.2024** . Dodávateľ súhlasí so zverejnením Zmluvy v celom jej znení vrátane jej prípadných príloh v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov v znení neskorších právnych predpisov (ďalej aj ako „Zákon“), pričom vyhlasuje, že táto Zmluva neobsahuje informácie, ktoré by nebolo možné zverejniť, resp.

sprístupniť v zmysle Zákona, a to najmä obchodné tajomstvo, bankové tajomstvo, daňové tajomstvo a pod. a v prípade, že také informácie obsahuje, dáva dodávateľ prevádzkovateľovi súhlas tieto informácie v zmysle Zákona zverejniť, resp. sprístupniť. V prípade, ak prevádzkovateľ nezverejní túto Zmluvu v zmysle Zákona a v zmysle § 47a Občianskeho zákonníka v lehote troch mesiacov odo dňa uzatvorenia tejto Zmluvy, platí, že k uzatvoreniu tejto Zmluvy nedošlo a Zmluvné strany nie sú touto Zmluvou viazané.

2. Táto Zmluva sa uzatvára na dobu určitú a to po dobu platnosti a účinnosti Zmluvy na výkon činností.

3. Počas platnosti a účinnosti Zmluvy na výkon činností je možné ukončiť túto Zmluvu dohodou zmluvných strán, alebo výpoveďou zo strany prevádzkovateľa bez udania dôvodu. Výpovedná lehota je tri mesiace a začne plynúť prvý deň nasledujúceho mesiaca po mesiaci, v ktorom bola písomná výpoveď doručená druhej zmluvnej strane. Skončenie tejto Zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie majú trvať aj po skončení platnosti tejto Zmluvy a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto Zmluvy, ku ktorému dôjde do skončenia platnosti tejto Zmluvy.

4. V prípade každého jednotlivého porušenia ktorejkoľvek povinnosti dodávateľa, vyplývajúcej z tejto Zmluvy, má prevádzkovateľ povinnosť žiadať voči dodávateľovi zaplatenie zmluvnej pokuty vo výške 5.000,-EUR (slovami: päťtisíc eur) a to za každé takého porušenie príslušnej povinnosti.

5. Prípadné ustanovenia o zmluvných sankciách uvedených v Zmluve na výkon činností týmto nie sú dotknuté.

6. Zmluvná pokuta je splatná na základe výzvy prevádzkovateľa na zaplatenie zmluvnej pokuty v lehote 14 (štrnásť) dní odo dňa jej doručenia dodávateľovi.

7. Nárok prevádzkovateľa na náhradu škody voči dodávateľovi, aj vo výške presahujúcej zmluvnú pokutu, nie je ustanoveniami o dojednaní zmluvnej pokuty, uplatnením zmluvnej pokuty voči dodávateľovi ani jej zaplatením dodávateľom dotknutý.

8. Ak vznikne prevádzkovateľovi ujma z dôvodu pochybenia dodávateľa, ktorý poruší svoje povinnosti dojednané touto Zmluvou alebo uložené mu právnymi predpismi, a to tak, že prevádzkovateľ bude na základe alebo v súvislosti s takou skutočnosťou zodpovedný za správny delikt v oblasti kybernetickej bezpečnosti alebo ochrany osobných údajov, vzniká prevádzkovateľovi nárok na náhradu takejto ujmy voči dodávateľovi v plnom rozsahu, vrátane prípadných ďalších vynaložených nákladov, vrátane nákladov za právne zastúpenie.

9. Právne vzťahy neupravené touto Zmluvou sa riadia ustanoveniami Obchodného zákonníka, zákona o kybernetickej bezpečnosti a jeho vykonávacími predpismi, prípadne inými všeobecne záväznými platnými právnymi predpismi Slovenskej republiky.

10. Zmluvné strany sa dohodli, že prípadné spory vyplývajúce z tejto Zmluvy budú riešiť predovšetkým vzájomným rokovaním zástupcov zmluvných strán, v prípade pretrvávajúcich sporov vzniknutých z tohto zmluvného vzťahu bude na konanie príslušný vecne a miestne príslušný súd Slovenskej republiky.

11. Zmeny a doplnenia tejto Zmluvy možno uskutočniť len na základe dohody zmluvných strán písomným a očíslovaným dodatkom k tejto Zmluve.

12. Ak ktorékoľvek ustanovenie tejto Zmluvy je alebo sa kedykoľvek stane nezákonným, neplatným alebo nevykonateľným v akomkoľvek ohľade, zákonnosť a vykonateľnosť zostávajúcich ustanovení tejto Zmluvy tým nebude dotknutá ani narušená. Zmluvné strany sa týmto zaväzujú rokovať o nahradení akéhokoľvek nezákonného, neplatného alebo nevykonateľného ustanovenia novými, pričom tieto nové ustanovenia sa budú čo najviac blížiť významu nezákonných, neplatných alebo nevykonateľných ustanovení.

13. Neoddeliteľnou súčasťou tejto Zmluvy je:
Príloha č. 1 – Štandard kybernetickej bezpečnosti v Slovenskej záručnej a rozvojovej banke, a. s.,

14. Táto Zmluva sa vyhotovuje v štyroch rovnopisoch, po dva pre každú zmluvnú stranu.

15. Zmluvné strany vyhlasujú, že túto Zmluvu pred jej podpísaním prečítali, že bola uzatvorená po vzájomnej dohode, podľa ich slobodnej vôle a nie v tiesni, ani za inak nápadne nevýhodných podmienok.

V Bratislave, dňa

Za prevádzkovateľa:

Ing. Radko Kuruc, PhD.
predseda predstavenstva
Slovenská záručná a rozvojová banka, a.s.

Ing. Pavel Mockovčiak
člen predstavenstva
Slovenská záručná a rozvojová banka, a.s.

V Bratislave, dňa

Za dodávateľa:

Mario Háronik
konateľ
Aricoma Systems s.r.o.

Príloha č. 1

Štandard kybernetickej bezpečnosti v Slovenskej záručnej a rozvojovej banke, a. s.

1. Úvod

Informačné systémy, technológie a prostriedky používané v SZRB musia byť zabezpečené takým spôsobom, aby sťažovali kompromitáciu infraštruktúry a aby v prípade kompromitácie služby alebo systému boli dôsledky incidentu minimalizované. To znamená, že ak útočník kompromituje časť infraštruktúry, je pre neho zložité dostať sa ďalej a kompromitovať ďalšiu časť infraštruktúry – to znamená je obmedzená možnosť pivotingu. Je nutné implementovať viacúrovňovú hĺbkovú ochranu – to znamená že bude bezpečnostná kontrola na viacerých miestach a prelomením jednej úrovne nedôjde priamo ku kompromitácii dát.
Vzhľadom na neustále sa vyvíjajúce a meniace techniky útokov a obrany je táto metodika žijúcim dokumentom.

1.1. Cieľ dokumentu

Tento dokument vyberá a sumarizuje minimálne bezpečnostné zásady a opatrenia potrebné na zabezpečenie informačných systémov, technológií a infraštruktúry SZRB ako aj pre novovznikajúce či existujúce projekty, procesy, zmeny a ostatné aktivity majúce vplyv na bezpečnosť informačných systémov (BIS) v SZRB tak aby platili princípy uvedené v úvode.
V dokumente sa používajú kľúčové slová „musí“, „malo by byť“, „odporúča sa“. Tieto sú ohodnotením dôležitosti daného opatrenia s ohľadom na jeho implementačnú náročnosť.

Dokument vznikol na základe podkladov z originálu Metodiky zabezpečenia IKT verejnej správy v oblasti informačnej bezpečnosti, ktorého autorom je CSIRT.SK (MetodikaZabezpeceniaIKT_v2.1.pdf (gov.sk)) a zo Zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú musieť byť vypracované v projektovej dokumentácii, zmenovej dokumentácii a ostatných podkladových materiálov, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru bezpečnosti informačných technológií na validáciu.

1.2. Obmedzenia

Dokument sa v tejto verzií nezaoberá špecifickými požiadavkami na: fyzickú bezpečnosť infraštruktúry, bezpečnosť mobilných zariadení, bezpečnosť Internetu vecí (IoT – Internet of Things), bezpečnosť ICS systémov (Industrial Control Systems), zabezpečenie služieb využívajúcich IPv4 multicast, zabezpečenie webových služieb (web services).

2. Štandardy implementácie

2.1. Bezpečnosť životného cyklu

Pri vývoji riešenia je potrebné myslieť na bezpečnosť už od začiatku a prispôsobiť tomu návrh aj implementáciu samotného riešenia počas jednotlivých fáz.

2.2. Návrh riešenia

Navrhnuté riešenie musí mať modulárnu štruktúru, pričom pri návrhu jednotlivých komponentov riešenia musí byť splnený princíp least privilege a všetky entity (t.j. používatelia aj systémy) musia mať prístup iba k údajom / aktívam, ktoré pre svoju činnosť nevyhnutne potrebujú, architektúra riešenia by mala byť trojvrstvová – mala by pozostávať z prezentačných serverov, aplikačných serverov a databázových serverov, odporúčané je použitie overených návrhových vzorov, napr. MVC, resp. MVP.
Musia byť identifikované všetky súčasti (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:

- prístupového vektoru útočníka (lokálny prístup/sieť),
- náročnosti získania prístupu,
- potreby autentifikácie,
- dopadov úspešného útoku na dostupnosť, integritu a dôvernosť riešenia a údajov v ňom spracovávaných.

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.

2.3. Implementácia riešenia

Riešenie musí byť vyvíjané v bezpečnom vývojovom prostredí. Pri implementácii 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.

Pri písaní zdrojového kódu by mal byť použitý systém na verzionovanie, pričom:

- jednotlivé zmeny (commity) by mali byť digitálne podpísané privátnym kľúčom autora daného commitu,
- commity by mali mať zmysluplné popisy,
- mala by byť implementovaná automatická kontrola zdrojového kódu na prítomnosť chýb a testovanie po každom commite.
- nemali by byť použité funkcie/volania/nástroje, ktoré sú podľa ich dokumentácie v súčasnej dobe zastarané (angl. deprecated) alebo nebezpečné (angl. unsafe) a mali by byť nahradené odporúčanými alternatívami.

Počas vývoja riešenia musia byť povolené všetky bezpečnostné vlastnosti použitých nástrojov, najmä však:

- zapnuté všetky varovania a ochrany vývojových nástrojov,
- varovania vývojového prostredia.

Počas vývoja musí byť vedená vývojárska dokumentácia:

- dokumentácia musí obsahovať bližší popis kľúčových častí riešenia až na prípadné výnimky chránené obchodným tajomstvom; tieto výnimky však musia byť zaznamenané v dokumentácii,
- v dokumentácii musí byť zaznamenaná každá zmena oproti pôvodnej špecifikácií a jej dôvody a každá takáto zmena musí byť schválená objednávateľom.

Dokumentácia aj zdrojové kódy riešenia musia byť odovzdané objednávateľovi spolu so samotným riešením. Pokiaľ je súčasťou riešenia aj databáza obsahujúca dôverné údaje:

- autentifikačné údaje musia byť uložené iba v podobe 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:

- (úspešné aj neúspešné) prihlásenie a odhlásenie,
- (úspešné aj neúspešné) vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny,
- (úspešné aj neúspešné) pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie),
- (úspešné aj neúspešné) pokusy o kritické operácie, zaznamenávajú sa úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
- zaznamenávajú sa úspešné a neúspešné prístupy k log súborom,

- zaznamenávajú sa úspešné a neúspešné prístupy k systémovým zdrojom,
- zaznamenáva sa vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
- zaznamenávajú sa zmeny v prístupových oprávneniach,
- zaznamenáva sa aktivácia a deaktivácia bezpečnostných mechanizmov,
- zaznamenáva sa spustenie a zastavenie procesov,
- zaznamenávajú sa konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
- zaznamenáva sa spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
- zaznamenávajú sa významné aktivity v sieťovej komunikácii,
- zaznamenáva sa požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
- zaznamenávajú sa IP adresy pridelené prostredníctvom služby DHCP,
- záznamy v log súboroch obsahujú ku každej udalosti (ak je k dispozícii) čas a dátum udalosti,
- záznamy v log súboroch obsahujú ku každej udalosti identifikáciu používateľa,
- záznamy v log súboroch obsahujú ku každej udalosti identifikáciu zariadenia,
- záznamy v log súboroch obsahujú ku každej udalosti informáciu týkajúcu sa udalosti,
- záznamy v log súboroch obsahujú ku každej udalosti indikáciu úspešnosti, alebo zlyhania operácie,
- záznamy v log súboroch obsahujú ku každej udalosti pri sieťových službách zdrojovú IP adresa, cieľovú IP adresa, protokol, zdrojový port, cieľový port, na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií synchronizovaný prostredníctvom presného časového zdroja,
- záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.
- logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov,
- riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server.

2.4. Testovanie a verifikácia riešenia

Po ukončení vývoja musí prejsť aplikácia testovaním a verifikáciou:

- vývojári by mali overiť aspoň pomocou automatizovaných nástrojov štandardné zraniteľnosti,
- malo by prebehnúť minimálne testovanie vstupov (fuzzing) a kontrola práce s pamäťou (memory leaky, memory corruption),
- vývojári musia zabezpečiť realizáciu opatrení vyplývajúcich z analýzy rizík vypracovanej pri návrhu riešenia,
- musí byť vykonané penetračné testovanie externou organizáciou,
- zraniteľnosti a problémy zistené na základe testovania musia byť odstránené a ich oprava musí byť potvrdená opakovaným testovaním.

2.5. Nasadenie a prevádzka riešenia

Hotové riešenie s odstránenými nájdenými zraniteľnosťami musí byť nasadené v prostredí zabezpečenom na základe odporúčaní v kapitolách o zabezpečení služieb a infraštruktúry.

Musí byť zabezpečené pravidelné monitorovanie nových zraniteľností jednotlivých (najmä externých) súčastí riešenia a pravidelné aplikovanie bezpečnostných záplat vydaných vývojármi, resp. tretími stranami. Aplikovanie týchto záplat musí podliehať opatreniam uvedeným v smernici pre riadenie záplat.

Bezpečný návrh – Webové aplikácie

Aplikačný a databázový server by mali byť umiestnené v internej sieti neprístupnej z Internetu.
Kód musí byť udržiavaný, prehľadný a dokumentovaný.
Prezentačná vrstva musí byť oddelená od aplikačnej a databázovej vrstvy.

3. Konfigurácia aplikačného servera

3.1. Systém

Systémy, nainštalované aplikácie a frameworky musia byť pravidelne aktualizované z pohľadu bezpečnosti.

Používané verzie softvéru musia byť podporované, resp. im nesmie končiť podpora. Počas doby, kedy prebieha údržba, rozsiahlejšia alebo mimoriadna aktualizácia OS/SW a/alebo nasadzovanie bezpečnostných záplat, by mali byť webové servery oddelené od zvyšku siete organizácie alebo byť umiestnené v izolovaných sieťach.

Na serveri musia byť deaktivované všetky nepoužívané služby, frameworky, doplnky a funkcionality.

Na serveri musia byť zatvorené všetky nepotrebné porty.

Autentifikácia používateľov na OS servera musí zodpovedať nasledujúcim požiadavkám:

- nepotrebné implicitné účty musia byť odstránené alebo zneplatnené,
- neaktívne kontá musia byť zneplatnené.
- na serveri by mali byť nakonfigurované používateľské skupiny, kontrola prístupu a udeľovanie privilégií by mali byť pre konkrétnych používateľov riadené ich zaradením do týchto skupín,
- heslo ku kontu musí zodpovedať požiadavkám organizácie na komplexnosť hesiel a má byť znemožnený útok hádaním či hrubou silou.

Právo na vykonávanie systémových úkonov musí byť obmedzené na poverených administrátorov.

Lokálny administrátor musí byť unikátny pre každý server.

3.2. Server

Pri inštalácií servera a bezprostredne po nej by mali byť vykonané nasledovné kontroly a akcie:

- sw servera má byť inštalovaný na dedikovanom hostiteľskom zariadení alebo na dedikovanom virtualizovanom OS,
- musia byť aplikované dostupné záplaty a aktualizácie na eliminovanie známych zraniteľností,
- nepotrebné východzie účty vytvorené pri inštalácií by mali byť odstránené alebo vypnuté,
- zo servera majú byť odstránené testovacie a ukážkové súbory vrátane vykonateľných súborov a skriptov a dokumentácia výrobcu,
- zo servera musia byť odstránené všetky nadbytočné a nepotrebné súbory a zložky, obzvlášť konfiguračné súbory a zálohy, ladiace výstupy, dočasné súbory, nepotrebné zdrojové kódy a zálohy súborov,
- ladiace funkcionality (napríklad ASP.NET Application Trace) musia byť vypnuté,
- server musí zobrazovať v prípade chyby servera iba všeobecné chybové hlásenia,

3.3. Administrácia, logovanie a zálohovanie

Správcovské rozhrania na všetky služby musia byť dostupné iba z dôveryhodných lokalít (potrebná reštrikcia na lokálne siete).

Z produkčných systémov musia byť odstránené všetky testovacie a pôvodné účty.

Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom.

Webové správcovské rozhrania musia byť dostupné iba prostredníctvom SSL/TLS.

3.4. Na serveri musí byť aktívne logovanie:

- malo by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent,
- pre každý virtuálny host na fyzickom webserveri by mal existovať separátny log,
- v logoch musia byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná,
- logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii,
- na uchovávanie logov musí byť vyhradená dostatočná kapacita,
- logy by mali byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov,
- logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie.

3.5. Kontrola prístupu OS a servera

Proces servera aj proces backendovej databázy musí byť konfigurovaný tak, aby bežal pod unikátnym používateľským kontom s limitovanou množinou privilégií.

Pre externé skripty a programy, vykonávané ako časť obsahu webového servera by mal byť vytvorený samostatný priečinok (napr. JavaScript knižnice a pod).

Spúšťanie skriptov, ktoré nie sú výlučne pod kontrolou administratívneho konta, malo by byť zakázané (napr. vytvorením a kontrolou prístupu k separátnemu priečinku, obsahujúcom autorizované skripty).

3.6. Autentifikácia a autorizácia

Aplikácia využíva autentifikáciu Active directory.

Aplikácia musí pre všetky autorizačné mechanizmy implementovať politiku, pri ktorej je zakázané všetko, čo nie je explicitne povolené (default-deny).

Aplikácia musí vyžadovať autentifikáciu pre každú privilegovanú operáciu (napr. meno a heslo na prvotné prihlásenie, token).

Aplikácia musí implementovať autorizáciu a autentifikáciu na strane servera.

Musia byť odstránené všetky testovacie a pôvodné účty z produkčných systémov.

Pre všetky citlivé operácie musia byť implementované anti-CSRF tokeny, ktoré musia byť pri vykonaní operácie overované.

Pre webové aplikácie, ku ktorým je na prístup nutná autentifikácia, je nutné zabezpečiť, aby žiadna webová stránka, ktorá má byť prístupné až po autentifikácii, nebola dostupná bez vykonania kompletného procesu autentifikácie.

Autentifikácia musí prebiehať prostredníctvom protokolu HTTPS.

Aplikácia musí vyžadovať používanie silných hesiel.

V prípade použitia iniciálnych náhodne generovaných hesiel pre nového používateľa musí aplikácia pri prvom prihlásení vyžadovať zmenu tohto hesla, v súlade s definovanými pravidlami pre tvorbu hesiel.

Aplikácia musí umožňovať administrátorom i používateľom zmeniť ich heslo.

Aplikácia musí po zmene hesla vydať nový identifikátor relácie, cez ktorú zmena hesla nastala. Ostatné relácie príslušného používateľa musia byť zneplatnené.

Aplikácia by mala pri zmene hesla notifikovať používateľa prostredníctvom Out-Of-Band kanála.

Aplikácia musí uložené heslá hashovať prostredníctvom štandardných kryptografických hashovacích funkcií a musí používať salt reťazce.

Aplikácia musí implementovať funkcionalitu pre odhlásenie (log-out) aj pre automatické odhlásenie po istej dobe nečinnosti. Funkcia odhlásenia má byť jednoducho identifikovateľná a dostupná z každej stránky, prístupnej po autentifikácii.

Aplikácia musí po odhlásení zneplatniť všetky relácie daného používateľa.

Odporúča sa, aby aplikácia podporovala simultánne paralelné prihlásenie k jednému účtu iba z jednej verejnej IP adresy. Odporúča sa, aby aplikácia pri zmene verejnej IP adresy prihláseného používateľa požadovala reautentifikáciu.

Je nutné vytvárať log záznamy všetkých pokusov o autentifikáciu (log-in, log-out, neúspešný log-in, lockout konta, žiadosť o zmenu hesla).

Pre privilegované účty sa musia používať používateľské mená, ktoré nie je možné jednoducho dedukovať (napr. štandardné loginy ako admin, administrator, user a pod, názov alebo typ aplikácie, kombinácie uvedených a pod.).

Používateľské kontá by mali byť po určitej dobe nečinnosti znefunkčnené.

Každý používateľ a administrátor musia mať jedinečné ID.

Aplikácia nesmie umožniť vytváranie účtov s používateľským menom podobným administrátorským či servisným kontám. (admin, administrator, helpdesk, support a pod.).

3.7. Používateľské vstupy

Všetky používateľské vstupy musia byť kontrolované na strane servera prostredníctvom whitelistov alebo regulárnych výrazov v kontexte, v ktorom sú použité.

Aplikácia musí brať ako vstupy a primerane ošetrovať všetky používateľom ovplyvniteľné časti dopytu, vrátane HTTP hlavičiek, URL, Cookies a pod. Bez ošetrenia nesmú byť reflektované v odpovedi servera. Napríklad:

- aplikácia musí byť odolná voči HTTP Spitting/Smuggling útokom,
- aplikácia by mala byť odolná voči HTTP Parameter Pollution (HPP) útokom,
- aplikácia/webový server musí byť odolný voči Host Header útoku.

Aplikácia by mala používať parametrizované SQL požiadavky (queries), tzv. prepared statements.

Aplikácia nesmie na tvorenie SQL dotazov využívať používateľské vstupy bez ich dôkladnej kontroly a ošetrenia.

Aplikácia musí ošetrovať vstupy od používateľa pred ich použitím minimálne:

- 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 dopyte 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 (Server-Side Inclusion statements) príkazoch, ak je použitie SSI nutné a povolené,
- 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,
- aplikácia musí ošetrovať vstupy/dátové prúdy prechádzajúce medzi modulmi aplikácie.

3.8. Relácie

Aplikácia by mala používať CSRF tokeny o veľkosti aspoň 128 bitov.

Aplikácia by nemala povoliť požiadavky spôsobujúce zmenu údajov, alebo citlivú operáciu bez platného CSRF tokenu.

Aplikácia nesmie povoliť požiadavky na privilegované operácie bez platného CSRF tokenu.

Na generovanie CSRF tokenov musí aplikácia používať kryptograficky silný generátor pseudonáhodných čísel.

Pri prihlásení musí aplikácia znovu vygenerovať nový identifikátor relácie.

Identifikátor predchádzajúcej neautentifikovanej relácie musí byť zneplatnený.

Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia znovu vygenerovať identifikátor relácie.

Pri zmene prihlasovacích údajov (používateľské meno, heslo) musí aplikácia zneplatniť ostatné relácie príslušného používateľa.

Pre relačné (session) cookies musí aplikácia nastaviť Secure flag.

Pre relačné (session) cookies musí aplikácia nastaviť HttpOnly flag.

Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu doménu.

Pre relačné (session) cookies musí aplikácia nastaviť reštriktívnu cestu (path).

Pre generovanie relačných identifikátorov musí aplikácia používať kryptograficky silné generátory pseudonáhodných čísel.

Aplikácia by mala používať relačné identifikátory o veľkosti aspoň 128 bitov.

Aplikácia musí zamietať neznáme relačné identifikátory zo strany klienta.

Relačné identifikátory musí aplikácia prenášať iba cez zabezpečené pripojenia.

Aplikácia musí vynucovať periodickú exspiráciu a zneplatnenie relácií.

3.9. Obsah

Aplikácia by mala pre všetky poskytované zdroje explicitne definovať typ obsahu.

Aplikácia by mala pre všetky poskytované stránky definovať „character set“.

Zabezpečenie aktívneho obsahu (skripty, spustiteľné súbory):

- právo na čítanie a zápis do súborového systému by malo byť limitované alebo zakázané,
- mala by byť povolená žiadna alebo len limitovaná interakcia s inými programami,
- nemala by byť potrebná žiadna akcia so SUID privilégiami (OS UNIX/Linux),
- skripty by pri spúšťaní externých programov mali používať absolútne cesty alebo nepoužívať žiadne cesty a spoliehať sa na premennú PATH, pričom tá musí obsahovať len bezpečné adresáre,
- žiadne priečinky nesmú mať súčasne práva na zápis a vykonávanie,
- spustiteľné súbory by mali byť umiestnené vo vyhradených priečinkoch,
- SSI (Server-Side Inclusion) by mali byť zakázané, resp. nie je možné ich spúšťať.

3.10. Spracovanie XML

Aplikácia nesmie podporovať:

- XML External entity expansion,
- parsovanie XML External DTD,
- všetky nadbytočné alebo nebezpečné XML rozšírenia.

Aplikácia by mala používať XML parser, ktorý neexpanduje entity rekurzívne.

3.11. Rôzne

Aplikácia by nemala podporovať presmerovanie na používateľom poskytnuté externé umiestnenia.

Aplikácia by mala obmedziť (krížový) prístup k (cudzím) doménam prostredníctvom whitelistingu.

Ak je na riadenie prístupu medzi doménami používané CORS (Cross Origin Resource Sharing), konfigurácia by mala byť obmedzená na dôveryhodné domény. Napr. nemala by byť použitá direktíva Access-Control-Allow-Origin:*.

Ak aplikácia používa na kontrolu prístupu k zdrojom na externých doménach súbory crossdomain.xml a/alebo clientaccesspolicy.xml, obsah by mal mať obmedzený na nutné domény, porty a protokoly. Nemali by byť používané nadmerne voľné pravidlá s „*“. Crossdomain.xml a clientaccesspolicy.xml nesmú byť prístupné koncovému používateľovi.

Aplikácia by mala pre všetky funkcionality vyžadujúce veľa zdrojov (napríklad CPU čas) implementovať rate limiting.

Pri implementácii rate limitingu sa musí brať ohľad na predchádzanie neúmyselnému odopretiu služby.

4. Interná infraštruktúra a vývojové prostredie

Jednotlivé vrstvy (databázová, aplikačná, prezentačná) by mali byť umiestnené v separátnych segmentoch a komunikácia medzi nimi musí byť filtrovaná.

Jednotlivé servery musia byť hardenované minimálne v rozsahu:

- vypnuté všetky nepotrebné procesy a služby,
- implementovaný host-based firewall, ktorý kontroluje všetku komunikáciu IN aj OUT a je nakonfigurovaný na princípe „least privilege“,
- všetky administrátorské účty spĺňajú politiku hesiel pre administrátorské účty,
- servery a všetok softvér je aktualizovaný neodkladne minimálne raz za mesiac,
- na serveroch by malo byť implementované anti-malware riešenie, ktoré je centrálne spravované a centrálne logované,
- všetky servery majú nastavené lokálny NTP server ako autoritatívny zdroj času a pre preklad doménových mien na IP adresy používajú lokálne DNS servery,
- všetky zariadenia musia byť hardenované podľa odporúčaní výrobcu.

4.1. Vývojové prostredie

Vo vývojovom prostredí musia byť použité iba nástroje spĺňajúce nasledovné:

- musia byť získané legálnym spôsobom z dôveryhodných zdrojov,
- musia byť stále podporované výrobcom (t.j. výrobca poskytuje bezpečnostné aktualizácie) nástroja a nesmú byť označené ako zastarané,
- musia byť aktualizované neodkladne minimálne raz za mesiac a musia byť aplikované bezpečnostné záplaty vydané výrobcom nástroja.

Vo vývojovom prostredí (vývojárske nástroje a podporné informačné systémy vrátane použitých knižníc tretích strán), v ktorom bude vyvíjané riešenie, musia byť implementované tieto opatrenia:

- musia byť implementované príslušné opatrenia na zabezpečenie integrity vyvíjaného riešenia na základe najvyššej požadovanej úrovne ochrany dôvernosti, integrity a dostupnosti informácií, ktoré budú spracovávané vo vyvíjanom riešení,
- ak samotné vyvíjané riešenie obsahuje informácie, ktoré je potrebné chrániť z hľadiska dôvernosti, musia byť vo vývojovom prostredí implementované opatrenia na zaistenie dôvernosti na základe požadovanej úrovne ochrany dôvernosti týchto údajov.

4.2. Štandardy prepojenia

4.2.1. Sieťové protokoly

Štandardom sieťových protokolov je:

- podpora sieťového protokolu Internet Protocol vo verzii 4 (IPv4) s podporou sieťovej technológie Dual stack spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP) pre informačné systémy alebo sieťového protokolu Internet Protocol vo verzii 6 (IPv6) spolu s protokolmi Transmission Control Protocol (TCP) a User Datagram Protocol (UDP),
- používanie skupiny protokolov Internet Procotol Security (IPSEC) na zabezpečenie sieťových protokolov.

4.3. Prenos dát

Štandardom prenosu dát je:

- používanie protokolu File Transfer Protocol (FTP, FTPS) alebo protokolu Hypertext Transfer Protocol (HTTP, HTTPS),
- podpora chráneného prenosu dát cez kryptografický protokol Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group.

4.3.1. Špecifikácie prepojenia pomocou sieťových služieb

Štandardom špecifikácie prepojenia pomocou sieťových služieb je používanie Domain Name Services (DNS) ako hierarchickej služby name servera v centrálnych bodoch internetu.

4.3.2. Sieťová a komunikačná bezpečnosť

- aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov,
- na prenos informácií k tretím stranám uzatvorenie zmluvy o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami,
- všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu,
- vzdialený prístup do vnútornej siete SZRB musí podliehať autentifikácii a autorizácii, vyžaduje sa použitia dvojfaktorovej autentizácie od každého vzdialeného pripojenia do internej siete,
- zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni: časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a ich uchovávanie aspoň 4 (štyri) mesiace,
- na všetkých serveroch podporujúcich základné služby informačných technológií SZRB sa implementujú sondy detekcie a prevencie prieniku technológia HIPS,
- všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom,
- implementácia druhého sieťového firewallu, aby interné servery a klientske stanice boli vo vzťahu k externým sieťam chránené dvomi sieťovými firewallmi,
- implementácia manažmentu logov,
- implementácia DNSSEC a jeho využitie pre všetky externe dostupné služby,
- zabezpečenie prístupu používateľov k Internetu a k službám mimo siete SZRB cez proxy server a uchovávanie prístupových logov aspoň 6 (šesť) mesiacov,
- používanie výhradne interného DNS servera a uchovávanie logov DNS dopytov aspoň 4 (štyri) mesiace,
- uchovávanie logov o IP adresách pridelených prostredníctvom DHCP aspoň 6 (šesť) mesiacov,
- rozdelenie siete do jednotlivých segmentov podľa účelu, pričom v rovnakých segmentoch môžu byť len zariadenia s rovnakými požiadavkami na úroveň zabezpečenia,

- zabezpečenie logovania sieťových spojení s externými sieťami na sieťových prvkoch a to minimálne na úrovni: časová pečiatka, zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port a uchovávanie týchto logov aspoň 6 (šesť) mesiacov.

5. Adresárové služby

Štandardom adresárovej služby je:

- používanie aplikačného protokolu Lightweighted Directory Access Protocol vo verzii 3 (LDAP v3) na verejný prístup k adresárovým službám,
- používanie jazyka Directory Services Markup Language v2 (DSML v2),
- podpora kryptografického protokolu Transport Layer Security (TLS) aspoň vo verzii podľa osobitnej špecifikácie SOG-IS Crypto Working Group pri chránenom verejnom prístupe k adresárovým službám.

5.1. Štandardy integrácie dát

Opisný jazyk dátových prvkov – štandardom opisného jazyku dátových prvkov je používanie jazyka Extensible Markup Language (XML) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pre dátové prvky.

5.2. Prenos dátových prvkov

Štandardom prenosu dátových prvkov je používanie:

- jazyka schém XML Schema Definition (.xsd) najmenej vo verzii 1.0 podľa World Wide Web Consortium (W3C) na výmenu dátových prvkov,
- jazyka Extensible Markup Language (.xml) vo verzii 1.0 podľa World Wide Web Consortium (W3C) pri výmene dátových prvkov, a to s hodnotou atribútu pre deklaráciu menného priestoru spravidla v tvare referencovateľného identifikátora, pričom ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov, je možné namiesto Extensible Markup Language použiť dátový model Resource Description Framework (RDF) opísaný formátmi RDF/XML podľa World Wide Web Consortium (W3C) alebo JSON-LD; pri otvorených údajoch je možné použiť aj formát CSV alebo formát JavaScript Object Notation (JSON),
- znakovej sady Unicode Character Set (UCS) podľa technickej normy v 8 bitovom kódovaní UTF-8,
- transformačného jazyka XSL Transformations (XSLT) podľa World Wide Web Consortium (W3C) pri transformácii dátových prvkov,
- formátu Geography Markup Language (GML) pri výmene priestorových dátových prvkov,
- jazyka Web Ontology Language (OWL) pre ontológie, ak je cieľom automatizované spracovanie rozlišujúce význam obsahu dátových prvkov,
- jazyka Shapes Constraint Language (SHACL) podľa World Wide Web Consortium (W3C) pre validáciu dátového modelu Resource Description Framework (RDF).

5.3. Formáty kompresie súborov

Štandardom formátov kompresie súborov je prijímanie a čítanie všetkých doručených formátov kompresie súborov, ktorými sú:

- ZIP (.zip) vo verzii 2.0,
- TAR (.tar),
- GZIP (.gz),
- TAR kombinovaný s GZIP (.tgz, .tar.gz),
- RAR (.rar).

5.4. Dátové štandardy

Štandardom výmeny údajov je:

- používanie technických parametrov dátových prvkov podľa dátových štruktúr vo formáte Extensible Markup Language Schema Definition (XSD
- Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou,
- Informácie v transakciách informačných technológií alebo medzi informačnými technológiami sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti) certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.

6. Šifrovanie

Webový portál musí byť prístupný prostredníctvom protokolu HTTPS.

K webovému portálu by sa nemalo pristupovať prostredníctvom HTTP.

Identita webového portálu musí byť zabezpečená platným, dôveryhodným certifikátom vydaným na doménu na ktorej je dostupný webový portál.

Identita webového portálu by mala byť zabezpečená certifikátom s Extended Validation.

Webový portál nesmie používať nedôveryhodné alebo vypršané SSL/TLS certifikáty.

Údaje, ktoré sú citlivé z hľadiska integrity alebo dôvernosti sa musia prenášať iba prostredníctvom zašifrovaného spojenia SSL/TLS.

Citlivé údaje (zvlášť prihlasovacie údaje) musia byť prenášané výhradne prostredníctvom zašifrovaného kanála.

Webový portál by nemal vkladať nešifrované zdroje bez SSL/TLS do stránok používajúcich SSL/ TLS.

Pri informačných technológiách s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.

Pri informačných technológiách s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä elektronických dokumentov a technológií v nasledujúcich riadkoch:

- šifrovanie dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
- šifrovanie emailovej komunikácie prostredníctvom PGP alebo S/MIME,
- šifrovanie komunikačných kanálov na výmenu nešifrovaných dát,
- šifrovanie centrálnych úložísk,
- šifrovanie záloh.

6.1. Šifrovacie kľúče a protokoly

server nesmie podporovať protokoly SSLv2, SSLv3, TLS 1.0 a TLS 1.1.

server musí podporovať TLS 1.2.

server by mal podporovať TLS 1.3.

server by nemal podporovať šifry s kľúčom kratším ako 112 bitov a blokom kratším ako 64bitov.

server nesmie podporovať NULL ciphers a anonymný Diffie-Hellman algoritmus.

server nesmie podporovať tzv. Export (EXP) šifry.

Použité šifry a protokoly SSL/TLS by mali byť odolné voči známym typom útokov, ako napríklad: FREAK, BEAST (používanie TLS 1.2, pri TLS 1.0 nepoužívanie šifry s AES), BREACH (Pri SSL/TLS musí byť vypnutá http kompresia), POODLE, LOGJAM, TLS Crime (TLS kompresia by mala byť vypnutá).

Dĺžka kľúča asymetrickej šifry RSA, DSA v X.509 certifikáte musí byť aspoň 2048 bitov. Toto neplatí pre ECDSA, kedy na dosiahnutie vysokej bezpečnosti postačujú kratšie kľúče – napríklad 256 bitov.

X.509 certifikáty musia byť hashované bezpečnými hashovacími funkciami (napr. kvôli možnosti kolíznych útokov nesmie byť použitý algoritmus MD5).

Webový server by mal podporovať šifry, ktoré majú vlastnosť Perfect Forward Secrecy (PFS).

Webový server by nemal podporovať RC4, DES a 3DES.

Šifry s CBC módom by mali byť nahradené bezpečnejšími AEAD šiframi. Pri použití CBC šifier je potrebné použiť ďalšiu autentifikáciu, napríklad HMAC (hashovaný autentifikačný kód správ).

Pre všetky kryptografické operácie musia byť použité kryptograficky silné generátory pseudonáhodných čísel.

Konfiguráciu odporúčame otestovať v SSL/TLS teste.

Pri správe SSL/TLS je nutné sledovať a v konfigurácii reflektovať aktuálne odporúčania. V prípade použitia WAF/FW pre SSL/TLS preň platia všetky vyššie uvedené požiadavky.

7. Firewall

Všetky prepoje medzi segmentami a externými sieťami musia byť chránené firewallom a všetky spojenia (IN aj OUT) musia byť povoľované iba na princípe least privilege.

Smerom do externých sieti by mala byť povolená len špecifikovaná komunikácia (pre interné siete by to malo byť len HTTP a HTTPS).

8. Zabezpečenie iných služieb

Pre prístup k neštandardným službám, ktoré nie je možné hardenovať a zabezpečiť štandardným spôsobom (napr. TLS) sa odporúča využiť prístup cez VPN.

8.1. Zmluvné požiadavky na BIS obsahujú najmenej záväzok:

- plnenia určených požiadaviek a kritérií pre oblasť BIS pri dodávke predmetu zmluvy,
- ochrany informácií, ku ktorým je poskytnutý prístup,
- oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa BIS a ďalších opatrení a postupov BIS špecifických na plnenie predmetu zmluvy,
- riadenia a monitorovania prístupov do informačných technológií SZRB vrátane spôsobu a mechanizmu,
- možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
- oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií SZRB zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,

- spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
- zachovania úrovne BIS pri významných zmenách vrátane spôsobu a formy prechodu k inému dodávateľovi.

8.1.1. Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká BIS a posúdia sa najmä:
- kritické komponenty a prvky služby,
- možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
- možné riziká BIS vo vzťahoch medzi dodávateľmi a subdodávateľmi,
- ďalšie možné riziká BIS vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému dodávateľovi.

Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.

Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia BIS v SZRB.

Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.

Pre informačné technológie SZRB, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.

Zamedzenie prístupu tretích strán ku všetkým údajom v IS SZRB, ktoré sa považujú za aktíva, alebo umožnenie prístupu tretích strán k takýmto údajom len na základe zmluvy tak, aby nebola narušená bezpečnosť IS SZRB a bezpečnostná politika SZRB.

Vysvetlenie skratiek

ACL – Access Control List
AP – Access Point
BIS – Bezpečnosť informačných systémov
CSRF – Cross-Site Request Forgery
DHCP – Dynamic Host Configuration Protocol
DMZ – Demilitarized Zone - VLAN, v ktorej sú umiestnené servery poskytujúce služby do externej siete, ktorá je logicky oddelená od internej siete (komunikácia je fultrovaná sieťovým firewallom)
DNS – Domain Name System
DoS – Denial of Service
FW – Firewall
IB – Informačná bezpečnosť
ICS – Industrial Control System
IS – Informačný systém
MitM útok – Man in the Middle útok
MVC – návrhový vzor Model–View–Controller
MVP – návrhový vzor Model–View–Presenter
NAC – Network Access Control
NAP – Network Access Protection
NDP – Neighbor Discovery Protocol - protokol v IPv6, okrem iného, nahradzujúci ARP z IPv4
NTP – Network Time Protocol
OS – Operačný systém PVLAN – Private VLAN princíp least privilege
RDP – Remote Desktop Protocol
QoS – Quality of Service
Sieťový firewall – firewall umiestnený v sieti filtrujúci komunikáciu viacerých zariadení, prípadne sietí (nie lokálny firewall)
SNMP – Simple Network Management Protocol
SSO – Single Sign-On
UAC – User Access Control
VLAN – Virtual Local Area Network
VPN – Virtual Private Network
VOIP – Voice over IP
WAF – Webaplikačný firewall – špeciálny typ firewallu, prispôsobený na zabezpečenie webového servera. Ide o filter, plugin či zariadenie ktorý aplikuje set pravidiel na HTTP prevádzku.
Whitelisting – metóda kontroly prístupu k službám, ktorá povoľuje prístup iba špecifikovaným klientom a všetkým ostatným ho zakazuje
XSS – Cross-Site Scripting
SZRB – Slovenská záručná a rozvojová banka, a. s.