Ministerstvo dopravy

Samostatné oddělení interního auditu

Příloha č. 10 ke smlouvě S-192-110/210

Akční plán k nápravě nedostatků a zmírnění rizik zjištěných auditem

K auditu s názvem:	**Audit kybernetické bezpečnosti č. 1/2020**
Č. j.:	**5/2020-040-AUD/24**
Vedoucí aud. týmu:	[redacted]

Schválil:	**ministr dopravy**	
Jméno, příjmení:	doc. Ing. Karel Havlíček, Ph.D., MBA	Podpis: doc. Ing. Karel Havlíček, Ph.D., MBA v. r.
Dne:	01.02.2021	

Legenda:
vyplňuje SO 042

Číslo zjištění dle Zprávy o auditu	Míra význam-nosti	Název zjištění	Doporučení auditorského týmu	Opatření k nápravě navržené auditovaným subjektem	Funkce, jméno a příjmení odpovědné osoby	Termín plnění opatření	Evidenční číslo úkolu v GINIS
Zjištění č. 1	Vysoká	Nesoulad s požadavky při zaznamenávání bezpečnostních a provozních událostí	Doporučení č. 1.1: (O330) Revidovat nejednoznačné ustanovení BPI MD v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.1 Požadavky na auditní záznamy, tzn. uvést jednoznačné ustanovení v souladu s požadavky VKB § 22, odst. 2, písm. b). Má-li být část tvorby bezpečnostních a provozních záznamů řešena na úrovni infrastruktury namísto aplikace, je toto potřeba jasně vymezit v rámci odstavců 4.2 Monitorování uživatelských aplikací až 4.8 Monitorování bezpečnostních zařízení BPI MD a také v rámci dodávek služby infrastruktury důsledně prosazovat.	Opatření č. 1.1: Manažer kybernetické bezpečnosti vydá standard, který bude obsahovat jednoznačné ustanovení obsahující zejména požadavky § 22 odst. 2, písm. b) VKB, tzn.: - aplikace logují události v rozsahu požadovaném vyhláškou o kybernetické bezpečnosti - § 22 odst. 2, písm. b) VKB, - logy jsou "on-line" zasílány do SIEM O2.	[redacted]	31.12.2020	N/A
			Doporučení č. 1.2: (O110, O150, O160) Prosadit v lozích aplikací zaznamenávání bezpečnostních a provozních událostí v souladu s revidovanou BPI MD na základě výše uvedeného doporučení. V případě aplikace CRŘ postupovat v návaznosti na opatření č. 2.1 z auditu KB č. 1/2019 evidované v elektronickém systému spisové služby Acta jako úkol č. U-040ro-3/2020 (nastavení procesu bezpečnostního monitoringu infrastruktury a aplikace CRŘ).	Opatření č. 1.2: Po vydání standardu manažerem kybernetické bezpečnosti zahrnující požadavky na zaznamenávání bezpečnostních a provozních událostí dle § 22 odst. 2, písm. b) VKB, zajistí správci jednotlivých informačních systémů Ministerstva dopravy, aby v lozích aplikací probíhalo zaznamenávání bezpečnostních a provozních událostí v souladu s vydaným standardem.	[redacted]	31.12.2021	UMD 15/2021
Zjištění č. 2	Vysoká	Obsah bezpečnostních a provozních záznamů	Doporučení č. 2.1: (O330) Definovat jednotný standard pro tvorbu bezpečnostních záznamů s ohledem na specifika prostředí MD (webové aplikace, autentizační a autorizační služba JIP/KAAS, atp.). Na základě platné BPI MD vznést požadavek na správce autentizační a autorizační služby JIP/KAAS na uplatnění požadavků VKB (§ 22, odst. 2, písm. d) a předávání příslušných bezpečnostních událostí, respektive incidentů k řešení, respektive na vědomí.	Opatření č. 2.1: Manažer kybernetické bezpečnosti vydá standard pro tvorbu a vyhodnocování bezpečnostních záznamů.	[redacted]	31.12.2020	N/A
			Doporučení č. 2.2: (O110, O150, O160) Prosadit v aplikacích CRŘ, ADR, ISTP, RPSD, eTesty a ISDT zaznamenávání bezpečnostních a provozních událostí v souladu s definovaným standardem. V případě aplikace CRŘ postupovat v návaznosti na opatření č. 2.1 z auditu KB č. 1/2019 evidované v elektronickém systému spisové služby Acta jako úkol č. U-040ro-3/2020 (nastavení procesu bezpečnostního monitoringu infrastruktury a aplikace CRŘ).	Opatření č. 2.2: Po vydání standardu pro tvorbu a vyhodnocování bezpečnostních záznamů manažerem kybernetické bezpečnosti, zajistí správce CRŘ, ADR, ISTP, RPSD, eTesty a ISDT, aby v aplikacích probíhalo zaznamenávání bezpečnostních a provozních událostí v souladu s vydaným standardem.		31.12.2021	UMD 16/2021

Zjištění č. 3	Střední	Ochrana bezpečnostních a provozních záznamů	Doporučení č. 3.1: (O330) Vyžadovat vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) ze strany Manažera KB, minimálně v rozsahu § 22 pro informační systém CRŘ (v návaznosti na opatření č. 2.1 z auditu KB č. 1/2019 evidované v elektronickém systému spisové služby Acta jako úkol č. U-040ro-3/2020 – nastavení procesu bezpečnostního monitoringu infrastruktury a aplikace CRŘ. S ohledem na absenci organizačního opatření v podobě oddělení dodavatele a provozovatele informačního systému RPSD definovat požadavek na zasílání vybraných událostí, které jsou dle platné BPI MD považovány za bezpečnostní incident. Pro ostatní významné informační systémy definovat po zvážení míry rizika požadavky na vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) v rozsahu vybraných událostí, které jsou dle platné BPI MD považovány za bezpečnostní incident.	Opatření č. 3.1: Vzdálené logování do centrálního systému pro sběr logů (SIEM) bude zajištěno splněním úkolu uloženého všem správcům informačních systémů Ministerstva dopravy Výborem pro řízení kybernetické bezpečnosti na 6. zasedání dne 9. 6. 2020: • zajistit on-line ukládání auditních záznamů z aplikací v požadovaném rozsahu do jednotného úložiště (SIEM O2), • nastavit pravidla pro detekci „podezřelých událostí“ v oblasti práce s aplikací („aplikační korelační pravidla“).	[redacted]	UMD 17/2021
			Doporučení č. 3.2: (O110, O150, O160) Nastavit v aplikacích CRŘ a RPSD vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) v rozsahu požadovaných událostí. Pro ostatní významné informační systémy – ADR, ISTP, eTesty a ISDT – nastavit vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) v rozsahu dle požadavku Manažera KB.	Opatření č. 3.2: a) V aplikacích CRŘ a RPSD provedou správci (O 110 a O 160) nastavení vzdáleného logování událostí do centrálního systému pro sběr logů (SIEM) v rozsahu požadovaných událostí. b) V aplikacích ADR, ISTP, eTesty a ISDT provedou správci (O 110, O 150 a O 160) nastavení vzdáleného logování událostí do centrálního systému pro sběr logů (SIEM) v rozsahu dle požadavku Manažera kybernetické bezpečnosti.		a) UMD 18/2021 b) UMD 19/2021
Zjištění č. 4	Střední	Nepodporované verze protokolu TLS	Doporučení č. 4: (O110, O160) Postupovat dle pokynů ze strany pracovní skupiny INFRA a realizovat vypnutí nepodporovaných verzí 1.0 a 1.1 protokolu TLS v souladu s požadavkem. Není-li to s ohledem na požadavky aplikací technicky možné, nesoulad řídit formou výjimek v souladu s přílohou č. 6 Řízení výjimek BPI MD.	Opatření č. 4: Správci systémů ADR, ISDT a eTesty realizují vypnutí nepodporovaných verzí 1.0 a 1.1 protokolu TLS v souladu s požadavkem (úkolem) pracovní skupiny INFRA.		UMD 20/2021
Zjištění č. 5	Střední	Nevhodné kombinace algoritmů dohod na klíči a šifrování klíčů	Doporučení č. 5: (O330) Revidovat cílové nastavení kombinací algoritmů dohod na klíči a šifrování klíčů a prosadit ukončení použití algoritmu AES v módu CBC. Je-li nutná podpora starších verzí protokolu TLS, vynutit bezpečnou kombinaci algoritmů dohod na klíči a šifrování klíčů. Není-li to s ohledem na možnosti protokolu či požadavky aplikací technicky možné, nesoulad řídit formou výjimek v souladu s přílohou č. 6 Řízení výjimek BPI MD. Pro aplikace využívající autentizační a autorizační službu JIP/KAAS je třeba postupovat v souladu s provozovatelem informačního systému Czech POINT. Nevyhovující kombinace algoritmů dohod na klíči a šifrování klíčů používající AES v módu CBC – TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) s ECDH x25519 (ekvivalent 3072 bitů RSA) FS, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) s ECDH x25519 (ekvivalent 3072 bitů RSA) FS, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) s DH 2048 bitů FS a TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) s DH 2048 bitů FS – budou na testovacím prostředí odstraněny dne 7. 10. 2020. Na produkčním prostředí je jejich odstranění ohlášeno na leden 2021.	Opatření č. 5: a) Manažer kybernetické bezpečnosti stanoví formou standardu Ministerstvem dopravy akceptovatelné algoritmy (kryptografické prostředky) v souladu s doporučením NÚKIB. Pracovní skupina INFRA následně zajistí připravenost infratruktury na vypnutí neakceptovaných kryptografických prostředků. b) Správci jednotlivých aplikací zajistí připravenost jimi spravovaných systémů na vypnutí neakceptovaných kryptografických prostředků.		UMD 21/2021
Zjištění č. 6	Nízká	Nesoulad požadavků na fyzickou bezpečnost	Doporučení č. 6: (O330) Revidovat BPI MD, část VIII. Fyzická bezpečnost a ustanovení smlouvy o Poskytování služeb provozu infrastruktury pro informační systémy Ministerstva dopravy, ev. č. S-8-330/2017, č. j. 2/2017-330-SML, ze dne 16. 5. 2017 tak, aby bylo zřejmé, že opatření v oblasti fyzické bezpečnosti mají být prosazena nejen formálně.	Opatření č. 6: a) Manažer kybernetické bezpečnosti vydá standard, který bude určovat minimální požadavky na fyzickou bezpečnost. b) Manažer kybernetické bezpečnosti zajistí provádění pravidelných kontrol (ověření souladu s tímto standardem) v serverovně Ministerstva dopravy a v datových centrech O2 ITS.		N/A

Upozornění pro auditované subjekty:
V souladu se zněním § 31 odst. 1 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole) schvaluje tento dokument ministr, proto i jakékoli požadavky na jeho změny/úpravy podléhají jeho schválení (včetně termínů plnění opatření k nápravě). V případě požadavku na změnu Akčního plánu ze strany auditovaného subjektu je nutné s dostatečným předstihem, tj. **před uplynutím termínu** přijetí opatření, zaslat SO 042 odůvodněnou žádost o změnu Akčního plánu. Tato žádost musí být podána vedoucím auditovaného subjektu, a to vždy s písemným souhlasem přímých představených až do úrovně náměstka pro řízení sekce, a to výhradně prostřednictvím spisové služby GINIS.