Ministerstvo dopravy

Odbor interního auditu a kontroly
Č. j.: 5/2020-040-AUD/16

Zpráva o auditu kybernetické bezpečnosti č. 1/2020

Název interního auditu:	Audit kybernetické bezpečnosti
Audit plánovaný/operativní:	plánovaný
Auditované subjekty:	Odbor provozu silničních vozidel, Odbor ICT, Odbor silniční dopravy a Odbor agend řidičů
Cíl interního auditu:	Ověřit soulad nastavení SŘBI MD s požadavky VKB, ověřit splnění nápravných opatření z auditu kybernetické bezpečnosti č. 1/2019, zhodnotit kontrolní mechanismy kybernetické bezpečnosti, fyzickou bezpečnost a kryptografické prostředky (§ 16, 17, 22, 26 VKB)
Auditované období:	1. května 2019 až 1. května 2020
Vedoucí auditorského týmu:	[redacted]
Členové auditorského týmu:	
Doba provedení auditu:	2. června 2020 až 25. září 2020

Obsah:

SEZNAM ZKRATEK A ZAVEDENÝCH POJMŮ

ADR	Přeprava nebezpečných věcí
BPI MD	Bezpečnostní politika informací Ministerstva dopravy, č. j. 1/2019-330-BP/2
CRŘ	Centrální registr řidičů
EPS	Elektrická požární signalizace
eTesty	Aplikace pro testování nových řidičů a dopravců v rámci autoškol
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IS	Informační systém
ISDT	Informační systém Digitální tachograf
ISSDS	Informační systém o silniční a dálniční síti ČR
ISTP	Informační systém technických prohlídek (ve Vyhlášce uvedeno jako Centralizovaný informační systém STK)
JIP/KAAS	Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb
KB	Kybernetická bezpečnost
KII	Kritická informační infrastruktura
MD	Ministerstvo dopravy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
O 110	Odbor silniční dopravy
O 150	Odbor provozu silničních vozidel
O 160	Odbor agend řidičů
O 330	Odbor ICT
ORP	Obecní úřady obcí s rozšířenou působností (tzv. obcí III. stupně)
PCO HZS	Pult centrální ochrany hasičského záchranného sboru
PCO PČR	Pult centrální ochrany Policie České republiky
PZTS	Poplachový zabezpečovací tísňový systém
RPSD	Rejstřík podnikatelů v silniční dopravě
RSV	Registr silničních vozidel (v Usnesení vlády ze dne 14. prosince 2016 č. 1139 uveden jako Centrální registr vozidel)
SŘBI	Systém řízení bezpečnosti informací (Information Security Management System)
SIEM	Správa bezpečnostních událostí a incidentů (Security Information and Event Management System)
STK	Stanice technické kontroly vozidel
VIS	Významný informační systém

VKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

1. SHRNUTÍ

Auditorský tým provedl tento audit kybernetické bezpečnosti č. 1/2020 na základě pověření č. j. 5/2020-040-AUD/3 vydaného ministrem dopravy dne 2. 6. 2020.

Audit byl zaměřen na prověření nastavení SŘBI MD v souladu s požadavky VKB, ověření splnění nápravných opatření z auditu kybernetické bezpečnosti č. 1/2019, kontrolní mechanismy kybernetické bezpečnosti, fyzickou bezpečnost a kryptografické prostředky. Auditovaným obdobím byl květen 2019 až květen 2020.

Audit byl proveden v období od června 2020 do září 2020 u Odboru provozu silničních vozidel, Odboru ICT, Odboru silniční dopravy a Odboru agend řidičů.

1.1 HODNOCENÍ AUDITOVANÉ OBLASTI

MD má revidovanou bezpečnostní politiku informací (č. j. 1/2019-330-BP/2), která je závazným řídicím dokumentem.

O 330 ověřuje vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) pro aplikaci RSV. Na základě tohoto ověření bude vzdálené logování událostí z ostatních informačních systémů KII a VIS MD součástí služby bezpečnostní politiky – KL001 realizované O2 IT Services s.r.o. Aktuálně probíhá tvorba bezpečnostních záznamů dodavateli jednotlivých aplikací nejednotným způsobem, v některých případech bez vazby na infrastrukturu. Nejednoznačné ustanovení BPI MD v případě některých aplikačních logů zapříčinilo, že i nově implementovaný systém není v souladu s ustanoveními VKB.

Opatření v oblasti fyzické bezpečnosti – za účelem zamezení neoprávněného vstupu, zamezení poškození informačních aktiv a zajištění ochrany informačních aktiv na úrovni objektů a v rámci objektů – jsou prosazována v souladu s požadavky BPI MD. Jejich formální prosazení však v některých případech je na úkor efektivity.

O 330 vede v rámci pracovní skupiny INFRA úkoly v oblasti kryptografických prostředků. Stanovené termíny vypnutí nepodporovaných protokolů nebyly některými aplikacemi dodrženy. V rámci revidovaných nastavení algoritmů dohod na klíči a šifrování klíčů byly na produkčních prostředích ponechány nevhodné kombinace. Rovněž zapnutí nové verze komunikačního protokolu nebylo dosud realizováno.

Na základě výše uvedených skutečností je pro auditované oblasti udělen výrok „*s výhradou*“.

CELKOVÉ HODNOCENÍ auditované činnosti/ procesu/ systému	**ŠKÁLA**	**POPIS** stupňů škály **CELKOVÉHO HODNOCENÍ**
	Nevyhovující	Byla identifikována zjištění s kritickou mírou významnosti nebo řada zjištění s vysokou mírou významnosti. Významná rizika nejsou auditovaným subjektem ošetřena. Řídící, popř. kontrolní systém není zaveden nebo je nefunkční. Nelze dosáhnout ujištění o funkčnosti auditované činnosti/ procesu/systému.
X	**S výhradou**	Byla identifikována zjištění s vysokou mírou významnosti nebo řada zjištění se střední mírou významnosti. Některá významná rizika nejsou auditovaným subjektem ošetřena. Podstatné řídící, popř. kontrolní mechanismy nejsou zavedeny nebo nejsou dostatečně účinné. Lze dosáhnout pouze částečného ujištění o funkčnosti auditované činnosti/procesu/systému.
	Vyhovující	Byla identifikována pouze zjištění se střední mírou významnosti nebo řada zjištění s nízkou mírou významnosti. Významná rizika jsou auditovaným subjektem uspokojivě ošetřena. Podstatné řídící a kontrolní mechanismy jsou zavedeny a jsou zpravidla účinné. Bylo dosaženo uspokojivého ujištění o funkčnosti auditované činnosti/procesu/systému.
	Standardní	Byla identifikována pouze zjištění s nízkou mírou významnosti. Rizika jsou auditovaným subjektem adekvátně ošetřena. Potřebné řídící a kontrolní mechanismy jsou zavedeny a jsou účinné. Bylo dosaženo uspokojivého ujištění o funkčnosti auditované činnosti/procesu/systému.

1.2 PŘEHLED ZJIŠTĚNÍ

POČET identifikovaných **ZJIŠTĚNÍ**	**Míra významnosti jednotlivých zjištění**	**POPIS** míry významnosti **JEDNOTLIVÝCH ZJIŠTĚNÍ**
0	Kritická	Zjištění kritické významnosti se zásadním dopadem na funkčnost auditované činnosti/procesu/systému. Zjištění je systémového charakteru.
2	Vysoká	Zjištění vysoké významnosti s významným dopadem na funkčnost auditované činnosti/ procesu/systému. Zpravidla se jedná o zjištění systémového charakteru.
3	Střední	Zjištění střední významnosti s dílčím dopadem na funkčnost auditované činnosti/ procesu/systému. Zpravidla se jedná o zjištění systémového nebo opakujícího se charakteru.
1	Nízká	Zjištění nízké významnosti se zanedbatelným dopadem na funkčnost auditované činnosti/ procesu/systému. Zjištění není systémového charakteru.

Jednotlivá zjištění jsou seřazena dle míry jejich významnosti od nejvýznamnějších k nejméně významným.

Číslo zjištění	**Název zjištění**	**Útvary dotčené zjištěním a doporučením**	**Míra významnosti**
1.	Nesoulad s požadavky při zaznamenávání bezpečnostních a provozních událostí	O 110 O 150 O 160 O 330	**vysoká**
2.	Obsah bezpečnostních a provozních záznamů	O 110 O 150 O 160 O 330	**vysoká**
3.	Ochrana bezpečnostních a provozních záznamů	O 110 O 150 O 160 O 330	**střední**

4.	Nepodporované verze protokolu TLS	O 110 O 160	**střední**
5.	Nevhodné kombinace algoritmů dohod na klíči a šifrování klíčů	O 330	**střední**
6.	Nesoulad požadavků na fyzickou bezpečnost	O 330	**nízká**

Podrobný popis zjištění včetně identifikovaných rizik, doporučení auditorů, stanovisek auditovaných subjektů a reakce auditorů je uveden v části **4. Zjištění, doporučení a stanoviska auditovaných subjektů včetně reakce auditorů.**

Opatření k nápravě k jednotlivým zjištěním a doporučením budou uvedena v Akčním plánu, který bude po schválení ministrem nedílnou součástí Zprávy o auditu kybernetické bezpečnosti č. 1/2020.

2. ÚVOD DO AUDITOVANÉ OBLASTI

Audit kybernetické bezpečnosti č. 1/2020 ověřoval na systémech tvořících KII MD (CRŘ, RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT):

- kontrolní mechanismy kybernetické bezpečnosti v rozsahu bezpečnostních opatření dle § 22 VKB,
- fyzickou bezpečnost v rozsahu bezpečnostních opatření dle § 17 VKB,
- kryptografické prostředky v rozsahu bezpečnostních opatření dle § 26 VKB.

Ověření bezpečnostních opatření v rozsahu organizačních opatření dle § 16 VKB (požadavky na audit KB) bylo, s ohledem na nemožnost zajištění principu nezávislosti interních auditorů na činnostech, které auditují, provedeno formou samostatného vyhodnocení. Toto vyhodnocení není zahrnuto v auditu kybernetické bezpečnosti č. 1/2020, nýbrž bude předáno ve formě Informace s hodnocením této oblasti ministru dopravy a na vědomí také předsedovi Výboru pro řízení kybernetické bezpečnosti.

Oblast výkonu kontrolních mechanismů kybernetické bezpečnosti v rozsahu bezpečnostních opatření podle § 22 VKB v prostředí MD upravují přílohy č. 4 Pravidla pro provozovatele IS a č. 6 Řízení výjimek BPI MD.

Oblast opatření fyzické bezpečnosti v prostředí MD upravují BPI MD a Směrnice č. 1/2014 Směrnice k zajištění bezpečnostní ochrany objektu Ministerstva dopravy, účinná dne 10. 3. 2014, č. j. 167/2013-030-BEZP/17.

Oblast opatření kryptografické prostředky v prostředí MD upravují přílohy č. 4 Pravidla pro provozovatele IS a č. 6 Řízení výjimek BPI MD. Dále jsou v řídicí dokumentaci odkazována aktuální doporučení Národního úřadu pro kybernetickou a informační bezpečnost.

Dodavatelé zajišťující vývoj aplikací tvořících KII MD (CRŘ, RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT) jsou odděleni od jejího provozovatele, kterým je O2 IT Services s.r.o., avšak s výjimkou CRŘ a RPSD. Postupy pro provoz se řídí dokumentem Pravidla zajištění provozu infrastruktury a service desku, verze 6.0 ze dne 7. 5. 2020.

Správu a rozvoj KII a VIS MD zajištují v rámci svých agend věcné odbory (O 110, O 150 a O 160) na základě smluv prostřednictvím dodavatelů uvedených v následující tabulce:

Název IS	Číslo smlouvy	Dodavatel
CRŘ	S-4-330/2007 (č. j. 37/2006-330-ORG/92)	ICZ a.s.
RSV	S-91-150/2017 (č. j. 31/2017-150-IS/1)	ICZ a.s.
ADR	S-9-110/2016 (č. j. 91/2016-110-SDNA)	CENDIS, s.p.
ISTP	S-346-150/2018 (č. j. 31/2018-150-IS)	AutoCont CZ a.s.
RPSD	S-268-110/2019 (č. j. 141/2019-110-SP/3)	CENDIS, s.p.
eTesty	014/2018/UNI_CEN_SLU (č. j. není přiděleno)	CENDIS, s.p.
ISDT	S-186-330/2016 (č. j. 15/2016-330-SML)	Státní tiskárna cenin, s.p.

2.1 PŘEDPISOVÁ ZÁKLADNA

- prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018, kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný
- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů
- vyhláška č. 416/2004 Sb., kterou se provádí zákon č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů
- vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
- vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích
- řád č. 4/2018 - Organizační řád, č. j. 57/2018-010-ORG/2 (pro zaměstnance mimo služební poměr)
- služební předpis č. 18 státního tajemníka Ministerstva dopravy ze dne 17. prosince 2019, změna č. 3, Organizační řád (pro státní zaměstnance)
- směrnice č. 1/2014 Směrnice k zajištění bezpečnostní ochrany objektu Ministerstva dopravy
- Bezpečnostní politika informací Ministerstva dopravy ze dne 18. 6. 2019, č. j. 1/2019-330-BP/2

2.2 AUDITORSKÉ POSTUPY

Pro účely auditu byly využity zejména následující postupy přezkoumávání a vyhodnocování operací a účinnosti vnitřního kontrolního systému:

- analýza,
- testování – test shody (soulad či nesoulad s danými ustanoveními VKB a BPI MD), test věcné správnosti (úplnost, přesnost, platnost informací),
- porovnávání a kontrolní skeny,
- šetření a ověřování,
- rozhovory.

Při výkonu auditu bylo postupováno v souladu se zákonem o finanční kontrole, se Směrnicí č. 5/2010 Statut a postupy interního auditu Ministerstva dopravy a byly zohledněny Mezinárodní standardy pro profesní praxi interního auditu (vydané mezinárodním institutem The Institute of Internal Auditors Inc. a do českého jazyka přeložené Českým institutem interních auditorů).

3. PROVEDENÁ PRÁCE

Bezpečnostní opatření jednotlivých IS byla auditorským týmem hodnocena v rozsahu rámce bezpečnostních opatření vyžadovaných zákonem o kybernetické bezpečnosti a vyhláškou o kybernetické bezpečnosti.

Ověřování zavedení procesů systému řízení bezpečnosti informací bylo zaměřeno na kontrolní mechanismy kybernetické bezpečnosti, fyzickou bezpečnost a kryptografické prostředky. V rámci posuzování souladu vykonávaných činností se auditorský tým zaměřil na porovnání aktuálního stavu vnitřních postupů MD a konkrétní realizace postupů na systémech tvořících KII MD (CRŘ, RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT) s požadavky stanovenými zákonem o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti.

U každé prověřované oblasti byly posuzovány následující čtyři aspekty:

1. pochopení a komunikace problematiky;
2. definice pravidel;
3. související procesy a implementace pravidel;
4. sledování účinnosti zásad a souvisejících procesů a postupy pro zlepšování.

Na základě hodnocení jednotlivých aspektů byla v prověřovaných oblastech zhodnocena efektivnost nastavených procesů systému řízení informační bezpečnosti.

3.1 POPIS AUDITOVANÉ OBLASTI

3.1.1 Kontrolní mechanismy kybernetické bezpečnosti

Ověřovány byly bezpečnostní opatření v rozsahu technických opatření dle § 22 VKB:

- způsob reakce na zaznamenané události a spolupráce provozovatele aplikací s dodavateli zajišťujícími vývoj při jejich řešení,
- způsoby zaznamenávání bezpečnostních a provozních událostí,
- informace zajištěné při zaznamenávání bezpečnostních a provozních událostí,
- doba uchovávání pořízených dat.

Požadavky na obsah, způsob tvorby a zpracování bezpečnostních a provozních událostí provozovatelem specifikuje příloha č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019, smlouvy 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 takto:

- *„zajistit trvalý vzdálený přístup k systémovým logům pro jednotlivé komponenty infrastruktury souvisejících s poskytovaným plněním a zamezit neoprávněnému přístupu třetích stran k záznamům týkajících se systémů,*
- *zajistit nástroj pro zaznamenávání činností komponent vztahujících se k předmětu plnění zaznamenaných do systémových logů způsobem, který zaznamenává nejméně:*
  - *přihlášení a odhlášení uživatelů a administrátorů,*
  - *činnosti provedené administrátory,*
  - *činnosti vedoucí ke změně přístupových oprávnění,*

  - *neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,*
  - *zahájení a ukončení činností systémů,*
  - *automatická varovná nebo chybová hlášení systémů,*
  - *přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností,*
  - *použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení*
- *na žádost poskytnout podklady (logy) a spolupráci pro analýzu provozu a incidentů automatizovanými nástroji,*
- *zajistit bezpečnostní dohled prostřednictvím SIEM zajistí zejména:*
  - *zaznamenávání činnosti infrastruktury (síťová infrastruktura, hardware, operační systémy, databáze, virtualizace, případně další), na které jsou provozovány informační systémy MD,*
  - *zaznamenávání údajů o komunikaci informačních systémů MD na perimetru DC,*
  - *zaznamenávání údajů činnosti informačních systémů MD na provozované infrastruktuře,*
  - *detekci kybernetických bezpečnostních událostí na základě výše uvedených záznamů,*
  - *upozornění na výskyt bezpečnostních událostí v reálném čase,*
  - *podporu pro vyhodnocení a analýzu bezpečnostních událostí s cílem rozhodnout, zda jde o bezpečnostní incident, tj. událost, která znamená ohrožení bezpečnosti informačního systému MD.*
- *zajistit vzdálený administrátorský přístup způsobem, který zajistí logování činností administrátorů.“*

Bezpečnostní záznamy technických aktiv jsou tvořeny a zpracovávány provozovatelem dle Pravidel zajištění provozu infrastruktury a service desku, verze 6.0 ze dne 7. 5. 2020. Vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) je ověřováno pro aplikaci RSV. Dodavatelé zajišťující vývoj aplikací tvořících KII MD (CRŘ, RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT) jsou odděleni od jejího provozovatele, kterým je O2 IT Services s.r.o., avšak s výjimkou CRŘ a RPSD (viz Zjištění č. 3).

Aplikace vytvářející auditní záznamy v databázích na platformě MS SQL využívají časový údaj bez časového pásma (viz Zjištění č. 1). Aplikace tvořící KII MD (CRŘ, RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT) jsou navrženy jako webové a nezaznamenávají události o odhlášení uživatele, dojde-li k němu v důsledku ukončení spojení klienta se serverem po uplynutí předem stanoveného intervalu (viz Zjištění č. 2). Aplikace využívající autentizační a autorizační službu JIP/KAAS - CRŘ, RSV a v konkrétních situacích i ISTP, RPSD, eTesty a ISDT – rovněž nezaznamenávají informaci o neúspěšných pokusech o přihlášení ze strany uživatele či administrátora.

Na základě předložené dokumentace byly údaje v bezpečnostních záznamech ověřovány na interview:

- s pracovníky O2 IT Services s.r.o. dne 3. 8. 2020 v 10:00,
- s pracovníky Státní tiskárny cenin, s.p. k aplikaci ISDT dne 5. 8. 2020 v 13:00,

- s pracovníky ICZ a.s. k aplikaci CRŘ dne 20. 8. 2020 v 13:00,
- s pracovníky CENDIS, s.p. k aplikaci RPSD dne 21. 8. 2020 v 9:00,
- s pracovníky CENDIS, s.p. k aplikaci eTesty dne 24. 8. 2020 v 12:00,
- s pracovníky CENDIS, s.p. k aplikaci ADR dne 24. 8. 2020 v 14:00,
- s pracovníky ICZ a.s. k aplikaci RSV dne 25. 8. 2020 v 13:00
- s pracovníky AutoCont CZ a.s. k aplikaci ISTP dne 3. 9. 2020 v 9:00.

3.1.2 Fyzická bezpečnost

Ověřována byla bezpečnostní opatření v rozsahu technických opatření dle § 17 VKB:

- předcházení poškození, zneužití nebo krádeži aktiv či přerušení poskytování služeb,
- stanovení fyzického bezpečnostního perimetru pro oblast uchovávání a zpracování informací a technických aktiv MD,
- přijetí nezbytných opatření a uplatnění prostředků fyzické bezpečnosti pro stanovený perimetr.

Požadavky na zajištění fyzické bezpečnosti informačních aktiv provozovatelem specifikuje příloha č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019, smlouvy 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 takto:

- *„umístit prostor DC na území České republiky, mimo zátopovou oblast a bezprostřední dosah produktovodů a jinak kritických míst,*
- *umístit hardware pro provoz infrastruktury do uzamykatelných skříní s řízeným přístupem,*
- *umožnit využít i rozvaděče třetích stran nebo zajistit provoz hardware třetích stran za identických smluvních podmínek,*
- *zajistit PZTS napojený na kamerový systém a systém kontroly vstupu,*
- *zajistit ochranu proti násilnému fyzickému vniknutí do prostor datového centra z prostor mimo datové centrum,*
- *zajistit 24 hodinovou ostrahu s PZTS napojeným na PCO PČR, bezpečnostní agentury či ekvivalentní formou dohledu,*
- *zajistit monitoring vstupu oprávněných osob do datového sálu v souladu s platnou legislativou,*
- *zajistit systém perimetrické ochrany datového sálu,*
- *zajistit ochranu proti požáru formou napojení na EPS s neustálým dohledem a hasicími plyny nepoškozujícími elektroniku,*
- *zajistit propojení systému EPS s PCO HZS nebo bezpečnostní agentury,*
- *zajistit monitoring teploty sálu a jednotlivých racků se vzdáleným přístupem pro oprávněné osoby,*
- *zajistit ochranu proti vytopení datového centra zevnitř (formou PZTS s neustálým dohledem),*
- *zajistit detekci zaplavení sálu,*
- *zajistit režim ostrahy a připojení výše uvedených systémů v režimu 24x7,*
- *zajistit způsob ostrahy znemožňující fyzický přístup nepovolaným osobám,*

- *zajistit řízený přístup k systémovým komponentám a to minimálně s ověřením ostrahou a kartou,*
- *zajistit logování událostí přístupového systému a uchování logů včetně logů PZTS, EPS (nejméně 6 měsíců) a záznamů kamerového systému (nejméně 1 měsíc)*
- *umožnit MD a jím určeným osobám přístup k záznamům kamerového systému a logům PZTS a EPS minimálně k nahlédnutí,*
- *zajistit nemožnost změny pořízených záznamů a logů,*
- *zajistit provozní podmínky zařízení pro poskytované služby dle doporučení výrobce.“*

Ověření proběhlo dne 5. 8. 2020 v 10:00 formou návštěvy datového centra Chodov společnosti O2 IT Services s.r.o. na adrese V lomech 2339/1, Praha 4. Auditorský tým byl datovým centrem proveden odpovědným zaměstnancem společnosti O2 IT Services s.r.o. Datové centrum je certifikováno Uptime Institutem na Tier III, částečně splňuje i požadavky Tier IV. Z opatření fyzické bezpečnosti jsou v budově prosazeny:

- PZTS,
- EPS,
- kamerový systém,
- přístupový systém,
- ostraha 24x7,
- napojení na PCO PČR
- napojení na PCO HZS,
- více faktorová autorizace osob HID kartou a PIN,
- uzamykatelné rozvaděče s možností individuální identifikace a kamerových okruhů (viz Zjištění č. 6).

V rámci datového centra Chodov jsou umístěna technická aktiva systémů tvořících KII MD (RSV) a VIS MD (ADR, ISTP, RPSD, eTesty, ISDT), a to v sálech na 1. NP a 3. NP. Oprávnění ke vstupu a režim návštěv upravuje Provozní řád datových center O2.

Technická aktiva systému CRŘ jsou umístěna pouze v datovém centru Nagano společnosti O2 IT Services s.r.o. na adrese K Červenému dvoru 25/3156, Praha 3. S ohledem na plánovaný přesun služeb do nového datového centra Stodůlky do konce roku 2020 nebyla návštěva datového centra Nagano realizována a skutečnosti byly ověřeny vůči předložené dokumentaci na interview:

- s pracovníky O2 IT Services s.r.o. dne 3. 8. 2020 v 10:00,
- s pracovníky ICZ a.s. dne 20. 8. 2020 v 13:00.

3.1.3 Kryptografické prostředky

Ověřována byla bezpečnostní opatření v rozsahu technických opatření dle § 26 VKB:

- použití odolných kryptografických algoritmů,
- použití systému správy klíčů a certifikátů,
- prosazování bezpečného nakládání s kryptografickými prostředky,

- zohledňování doporučení v oblasti kryptografických prostředků vydaná NÚKIB.

Požadavky na použití kryptografických prostředků provozovatelem specifikuje příloha č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019, smlouvy 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 takto:

- *„umožnit šifrování logických disků,*
- *umožnit šifrování databází,*
- *zajistit dodržení standardů bezpečnosti přístupu k šifrovacím klíčům a jejich pravidelnou obměnu,*
- *zajistit použití šifrovacích klíčů infrastruktury v souladu s požadavky zákona č. 181/2014 Sb. v platném znění a jeho prováděcími předpisy,*
- *zajistit bezpečnost přístupu k šifrovacím klíčům infrastruktury.“*

Požadavky na kryptografii jsou prosazovány pracovní skupinou INFRA. Aktuálně jsou realizovány úkoly Vypnutí TLS 1.1 a Povolení TLS 1.3. Některé z aplikací úkoly ze strany pracovní skupiny nerealizovaly v požadovaných termínech (viz Zjištění č. 4). Provedená revize nastavení kryptografických algoritmů ponechala na serverech nevhodné kombinace algoritmů dohod na klíči a šifrování klíčů (viz Zjištění č. 5).

Skutečnosti byly dne 27. 8. 2020 ověřeny kontrolními skeny serverů zaměřenými na algoritmy a verze protokolů využívané při navazování komunikace prostřednictvím webového prohlížeče:

- crv.mdcr.cz (IP adresa 185.17.215.21),
- crr.mdcr.cz (IP adresa 185.17.215.58),
- sod.mdcr.cz (IP adresa 185.17.215.42),
- istp.mdcr.cz (IP adresa 185.17.214.147),
- rpsd.mdcr.cz (IP adresa 185.17.215.27),
- etesty2.mdcr.cz (IP adresa 185.17.215.32),
- etadm2.mdcr.cz (IP adresa 185.17.215.34),
- dt.mdcr.cz (IP adresa 185.17.215.39).

Na základě předložené dokumentace a výsledku kontrolních skenů výše uvedených serverů byly skutečnosti taktéž ověřovány na jednotlivých interview, viz přehled uskutečněných schůzek v bodě 3.1.1.

4. ZJIŠTĚNÍ, DOPORUČENÍ A STANOVISKA AUDITOVANÝCH SUBJEKTŮ VČETNĚ REAKCE AUDITORŮ

Číslo zjištění:	1
Název zjištění:	Nesoulad s požadavky při zaznamenávání bezpečnostních a provozních událostí

Popis zjištění:

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, definuje v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.1 Požadavky na auditní záznamy, požadavky na strukturu auditních záznamů. Mimo vlastní auditní informaci je požadováno uvedení data a času (kdy k události došlo), identifikace uživatele (či automatu) a zdroj (IP adresa, lokální konzole a podobně).

VKB v § 22, odst. 2, písm. b) vyžaduje mimo jiné v auditním záznamu uvádět datum a čas včetně specifikace časového pásma, identifikaci technického aktiva zaznamenávajícího činnost a jednoznačnou síťovou identifikaci zařízení původce. **Ustanovení BPI MD tak není v souladu s požadavky VKB.**

Aplikace vytvářející auditní záznamy v databázích na platformě MS SQL využívají časový údaj obvykle reprezentovaný typem DATETIME resp. CURRENT_TIMESTAMP ve formátu RRRR-MM-DD HH:MM:SS.SSS. Toto je v souladu s požadavky BPI MD, nikoliv však VKB (§ 22, odst. 2, písm. b). Pro naplnění požadavku VKB je třeba využít volání funkce SYSDATETIMEOFFSET(), která vrací hodnotu data a času včetně časového pásma ve formátu RRRR-MM-DD HH:MM:SS.SSSSSSS ±PP:PP.

Rovněž informace o původci události se v databázových lozích různí s ohledem na nejednoznačný výklad BPI MD. Například ADR identifikuje v tabulce *adr_log* v poli *subject* pouze adresu serveru a metodu či volanou funkci kódu aplikace. Toto je v souladu s požadavky BPI MD, nikoliv však VKB (§ 22, odst. 2, písm. b). Naopak aplikace eTesty identifikuje v tabulce *ApplicationLog* v poli *ServerName* identifikaci technického aktiva zaznamenávajícího činnost a v poli *ClientInfo* IP adresu a údaje o použitém webovém prohlížeči. Jako jednoznačná identifikace klienta je brán údaj HTTP hlavičky X-Forwarded-For (XFF), obsahující identifikaci původní IP adresy klienta předávanou službou CMS2, kterou je zajištěna síťová konektivita pro aplikace MD.

Míra významnosti zjištění:	Vysoká
Identifikovaná rizika:	MD není schopno zaznamenávat kybernetické bezpečnostní události a incidenty v souladu s požadavky právních předpisů (VKB § 22, odst. 2, písm. b). V případě rozdílně nastavených časových zón či změny letního a zimního času může dojít při analýze zaznamenaných událostí k časovému posunu.

	Absence údaje o jednoznačné síťové identifikaci původce události znemožňuje validní reakci na případný kybernetický bezpečnostní incident.

Doporučení:

O 330

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.

O 110, O 150, O 160

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).

Stanoviska auditovaných subjektů:

Stanovisko O 110

Akce:

1. Provést kontrolu, zda jsou ukládány záznamy v auditních databázích včetně údaje časového offsetu časové zóny v souladu s VKB

Údaje jsou ukládány s časovou značkou včetně údajů o milisekundách, avšak bez uvedení časové zóny. Prosím o ověření, zda postačují údaje s časovou značkou bez časové zóny.

2. Zajistit logování IP adresy klienta na základě X-Forwarded-For (XFF) z http headeru

Bude řešeno za součinnosti s O330.

Stanovisko O 150

Pokud dojde k bližší specifikaci ustanovení BPI v části VI Bezpečnost provozu v kapitole 4 Monitorování, odstavce 4.1 Požadavky na auditní záznamy odborem O 330 bude O 150 realizovat změnu v souladu s novou specifikací. V této oblasti předpokládáme, že vše bude řešeno v rámci pracovních skupin RSV a IS TP, kde je O 330 členem.

Stanovisko O 160

IS Centrální registr řidičů (IS CRŘ)

Již od konce roku 2019 probíhá odesílání údajů z prostředí operačních systémů IS Centrální registr řidičů do SIEM za použití klienta dodaného provozovatelem SIEM,

jehož konfigurace byla provedena na základě návrhu/požadavku provozovatele SIEM. Z toho rovněž plyne, že pokud i v případě současně odesílaných logů z IS CRŘ je rozporován formát auditního záznamu (chybějící údaj o časovém pásmu), musí být tento rozpor vyřešen dodáním příslušného klienta pro odesílání záznamů do SIEM, popř. jeho konfigurace, což by mělo zajistit požadovaný formát časového údaje. Doposud jsou tedy auditní záznamy posílány z IS CRŘ do SIEM pouze na úrovni infrastruktury/operačních systémů a jejich obsah je plně v kompetenci klientské aplikace dodané provozovatelem SIEM a její konfigurace, tj. provozovatel ISCRŘ nemá možnost jejich konečný obsah a formu v SIEM ovlivnit.

IS CRŘ používá i s historickou návazností časové údaje typu „datetime“. Tento datový typ však neobsahuje údaj o časovém pásmu. Případná úprava tohoto mechanismu musí především navazovat na případné úpravy BPI MD a nelze ji tedy navrhnout a realizovat dříve, než O 330 přijme příslušná opatření/reviduje BPI MD. Vzhledem ke skutečnosti, že jsou všechny auditní záznamy z IS CRŘ generovány v rámci jediného a pevně daného časového pásma, navrhujeme snížení stupně výhrady, protože nám nepřijde pro výše uvedené adekvátní, popř. navrhujeme zvážit, zda se nedá věc řešit přímo na straně SIEM.

V současné době probíhá implementace úpravy IS CRŘ představující odesílání dalších aplikačních logů do SIEM (přihlašování uživatelů, manipulace s aplikačními účty a oprávněními).

<u>IS Digitální tachograf (IS DT)</u>

Případná úprava předmětného mechanismu u IS DT musí především navazovat na případné úpravy BPI MD a nelze ji tedy navrhnout a realizovat dříve, než O 330 přijme příslušná opatření/reviduje BPI MD.

<u>IS eTesty</u>

Případná úprava předmětného mechanismu u IS eTesty musí především navazovat na případné úpravy BPI MD a nelze ji tedy navrhnout a realizovat dříve, než O 330 přijme příslušná opatření/reviduje BPI MD.

Reakce auditorů/Závěr:

Auditorský tým na základě provedeného ověření potvrzuje, že údaj bez časového pásma není v souladu s požadavky legislativy. Závažnost zjištění byla stanovena s ohledem na nesoulad s požadavky legislativy a absenci jednotného standardu pro tvorbu bezpečnostních záznamů. Proto nelze návrhu O 160 na snížení stupně výhrady vyhovět. Tento nesoulad není řešen formou výjimky dle přílohy BPI MD Řízení výjimek. O 330 dle sdělení v rámci konzultací ke zjištěním obsaženým v Návrhu Zprávy o auditu kybernetické bezpečnosti č. 1/2020 předpokládá nastavení jednotného standardu pro tvorbu bezpečnostních záznamů, kde bude stanoven přesný formát času a případné možné úpravy v rámci zpracování bezpečnostních záznamů. Aktuální situace umožnuje realizaci výše uvedeného rizika chyby při analýze bezpečnostních záznamů.

V uvedených stanoviscích auditorský tým neidentifikoval důvody pro revizi zjištění.

Zjištění zůstává beze změny.

Číslo zjištění:	2
Název zjištění:	Obsah bezpečnostních a provozních záznamů

Popis zjištění:

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, definuje v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.2 Monitorování uživatelských aplikací, požadavky na tvorbu auditních záznamů a jejich sběr a vyhodnocování.

Aplikace CRŘ, RSV, ADR, ISTP, RPSD, eTesty a ISDT jsou navrženy jako webové. Pro přístup je využíván webový prohlížeč a s výjimkou aplikace ISTP nemají k dispozici tlustého klienta. V případě ISTP je klient určen pro STK v situaci nedostupnosti serverů aplikace a jeho použití musí být ze strany MD v konkrétní okamžik povoleno. V auditních záznamech aplikace není obsažena událost odhlášení uživatele, dojde-li k němu v důsledku ukončení spojení klienta se serverem po uplynutí předem stanoveného intervalu (do 30 minut v závislosti na způsobu použití dané aplikace).

Aplikace využívající autentizační a autorizační službu JIP/KAAS – CRŘ, RSV a v konkrétních situacích i ISTP, RPSD, eTesty a ISDT – rovněž nezaznamenávají informaci o neúspěšných pokusech o přihlášení ze strany uživatele či administrátora. Toto je dáno technickým omezením služby JIP/KAAS, kdy server MD automaticky přesměrovává uživatele na servery autentizační a autorizační služby JIP/KAAS, které neposkytují informaci o neúspěšných pokusech o přihlášení. V případech, kdy má ORP přiřazeného administrátora a správa oprávnění probíhá čistě v autentizační a autorizační službě JIP/KAAS, rovněž nejsou dostupné záznamy o úspěšných či neúspěšných manipulacích s účty, oprávněními a právy.

Bezpečnostní záznamy technických aktiv jsou tvořeny dle Pravidel zajištění provozu infrastruktury a service desku, verze 6.0 ze dne 7. 5. 2020. Odstavec 9 Syslog & SIEM popisuje zpracování bezpečnostních událostí a incidentů pro aplikace MD (mimo CRŘ) provozované na základě přílohy č. 1, odstavec 2 Služba technického provozu a poskytování virtuální infrastruktury – KL002 dodatku č. 2 smlouvy o Poskytování služeb provozu infrastruktury pro informační systémy Ministerstva dopravy, ev. č. S-8-330/2017, ze dne 16. 5. 2017. Ze strany dodavatelů aplikací nejsou, až na výjimky, analýzy problematických situací nijak zpracovávány.

Evidence výjimek v souladu s přílohou č. 6 Řízení výjimek BPI MD, neobsahuje konkrétní ustanovení o nesouladu obsahu bezpečnostních a provozních záznamů vůči požadavkům VKB § 22, odst. 2, písm. d).

Míra významnosti zjištění:	Vysoká
Identifikovaná rizika:	MD není schopno zaznamenávat kybernetické bezpečnostní události a incidenty v souladu s požadavky právních předpisů (VKB § 22, odst. 2, písm. d). V situaci, kdy útočník opakovaně neúspěšně zkouší přihlášení skrze autentizační a autorizační službu JIP/KAAS, tato skutečnost není ze strany MD zaznamenána a není na ni reagováno.

Doporučení:

O 330

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.

O 110, O 150, O 160

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).

Stanoviska auditovaných subjektů:

Stanovisko O 110

Akce:

1. Zajistit, aby při odhlášení klienta po timeoutu došlo k zaznamenání této události do auditních záznamů

Zajistit logování neúspěšných záznamů o přihlášení přes JIP/KAAS (JIP/KAAS aktuálně technicky toto řešení nenabízí, není tedy v gesci provozovatele).

Stanovisko O 150

Bude prosazeno zaznamenání bezpečnostních a provozních událostí, což bude projednáno a řešeno v rámci pracovních skupin RSV a IS TP002E

Stanovisko O 160

IS CRŘ

Mimo stanovisko související s vyjádřením ke zjištění č. 1 uvádíme, že IS CRŘ je při využití služeb JIP/KAAS schopno zaznamenat neúspěšné pokusy o přihlášení, avšak nikoliv klasické chybné zadání autentizačního údajů uživatelem na stránkách JIP/KAAS, což s ohledem na technologii nyní není možné, ale např. pokusy o neúspěšné přihlášení způsobené pokusem o podvržení autentizačních tokenů nebo jakékoliv další problémy, které rozhraní JIP/KAAS umožňuje při ověření autentizačního tokenu odhalit (např. jeho expirace).

IS CRŘ má vlastní správu uživatelů a údaje o přihlašování uživatelů, manipulaci s aplikačními účty a oprávněními tak do SIEM umožňuje (nyní je předmětem implementace právě prováděných úprav). JIP/KAAS řeší pouze autentizaci uživatelů a autorizace na jeho straně spočívá pouze v indikaci možnosti se do IS CRŘ přihlásit přes JIP/KAAS.

IS DT a IS eTesty

Dle vyjádření dodavatelů předmětných IS technologie JIP/KAAS dané možností chování nenabízí a není tedy v moci provozovatele dopravně správních agend tuto věc řešit. Je na zvážení O330, zda upraví BPI MD nebo zajistí s provozovatelem JIP/KAAS aktivaci nové funkcionality.

Domníváme se, že jelikož je JIP/KAAS používán napříč agendami státní a veřejné správy, mělo by již zcela jistě existovat nějaké auditní stanovisko k této problematice, např. na straně Ministerstva vnitra, které navrhujeme v tomto případě oslovit.

Reakce auditorů/Závěr:

V uvedených stanoviscích auditorský tým neidentifikoval důvody pro revizi zjištění.

Zjištění zůstává beze změny.

Číslo zjištění:	3
Název zjištění:	Ochrana bezpečnostních a provozních záznamů

Popis zjištění:

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, definuje v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.10 Logy o činnosti administrátorů a operátorů, požadavek na ochranu logů proti narušení ze strany privilegovaných uživatelů, je-li to technicky a organizačně možné.

MD prosazuje koncept ochrany organizačním opatřením, kdy dodavatelé zajišťující vývoj aplikace jsou odděleni od jejího provozovatele, kterým je O2 IT Services s.r.o., avšak s výjimkou CRŘ a RPSD.

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, definuje v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.9 Ochrana auditních záznamů, požadavek zajistit vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) na základě vyžádání Manažera KB.

Pracovní skupina INFRA vede úkol *Zvýšená oprávnění ICZ*, kdy jsou do SIEM začleňovány logy SQL databáze RSV. Logy z infrastruktury provozované O2 IT Services s.r.o. jsou zaznamenávány do centrálního systému pro sběr logů a jsou odděleny role administrátorů dle požadavků odstavce 4.9 Ochrana auditních záznamů. Dokument Pravidla zajištění provozu infrastruktury a service desku, verze 6.0 ze dne 7. 5. 2020, odstavec 9 Syslog & SIEM popisuje zpracování bezpečnostních událostí a incidentů pro aplikace MD (mimo CRŘ) provozované na základě přílohy č. 1, odstavec 2 Služba technického provozu a poskytování virtuální infrastruktury – KL002 dodatku č. 2 smlouvy o Poskytování služeb provozu infrastruktury pro informační systémy Ministerstva dopravy, ev. č. S-8-330/2017, ze dne 16. 5. 2017.

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, definuje v části VI. Bezpečnost provozu, kapitola 4 Monitorování, odstavec 4.1 Požadavky na auditní záznamy, požadavek na řešení výpadku auditních funkcí požadovaných BPI MD formou bezpečnostního incidentu.

Při interview s jednotlivými dodavateli aplikací nebylo prokázáno, že změna nastavení aplikace či vypnutí tvorby auditních záznamů je zaznamenáno. MD tak nemá možnost zjistit, že nastal bezpečnostní incident definovaný BPI MD. Některé z aplikací, např. ISTP, neumožňují záznamy v databázi mazat a koncepce oddělení rolí dodavatele a provozovatele aplikace je prosazována i na úrovni databázového oprávnění. Riziko neoprávněného zásahu do auditních záznamů je tak minimální a zbývá k řešení pouze riziko neoprávněného čtení.

Ochrana bezpečnostních a provozních záznamů organizačním opatřením, kdy dodavatelé zajišťující vývoj aplikace jsou odděleni od jejího provozovatele, je v uvedených případech neúčinná.

Míra významnosti zjištění:	Střední
Identifikovaná rizika:	MD není schopno zaznamenávat kybernetické bezpečnostní události a incidenty v souladu s požadavky právních předpisů (VKB § 22, odst. 2, písm. c). V situaci, kdy je držitelem privilegovaných oprávnění provedena změna nastavení aplikace pro zaznamenávané kybernetické bezpečnostní události a incidenty či je proveden do záznamů zásah, není tato skutečnost zjistitelná jako definovaná událost v rámci centrálního systému pro sběr logů.

Doporučení:

O 330

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.

O 110, O 150, O 160

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.

Stanoviska auditovaných subjektů:

<u>Stanovisko O 110</u>

Akce:

1. Integrovat IS RPSD na SIEM MD

Bude řešeno za součinnosti O330 a bude součástí chystané analýzy a následné úpravy celého systému.

Stanovisko O 150

Bude nastaveno vzdálené logování událostí do centrálního systému pro sběr logů (SIEM) podle požadavků v rozsahu Manažera KB, což bude projednáno a řešeno v rámci pracovní skupiny IS TP. Spíše se bude jednat o úpravu zabezpečující řešení neoprávněného čtení.

Stanovisko O 160

IS CRŘ

Viz vyjádření ke zjištění č. 1.

IS DT

Předmětná opatření jsou v současné době konzultována s dodavatelem, přičemž jsou předmětem jeho dílčí analýzy, jejíž součástí bude i vyhodnocení, v jakém rozsahu je opatření možné technicky realizovat a doporučené implementovat již do stávající verze systému.

IS eTesty

Předmětná opatření jsou v současné době konzultována s dodavatelem, přičemž jsou předmětem jeho dílčí analýzy, jejíž součástí bude i vyhodnocení, v jakém rozsahu je opatření možné technicky realizovat a doporučené implementovat již do stávající verze systému.

Reakce auditorů/Závěr:

V uvedených stanoviscích auditorský tým neidentifikoval důvody pro revizi zjištění.

Zjištění zůstává beze změny.

Číslo zjištění:	4
Název zjištění:	Nepodporované verze protokolu TLS

Popis zjištění:

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, odkazuje v části V. Kryptografická opatření, kapitola 2 Symetrické algoritmy, asymetrické algoritmy a hashovací funkce, na aktuální doporučení Národního úřadu pro kybernetickou a informační bezpečnost a nesoulad má být řízen formou výjimek v souladu s přílohou č. 6 Řízení výjimek BPI MD.

Pracovní skupina INFRA vede úkol Vypnutí TLS 1.1 a nižší, kdy všem odborům byl směrován požadavek vypnutí do 30. 3. 2020. Na nutnost vypnutí

zastaralých protokolů byli provozovatelé IS upozorněni dne 21. 6. 2019 elektronickou poštou ze strany manažera kybernetické bezpečnosti MD.

Servery VIS eTesty a ISDT – etesty2.mdcr.cz (IP adresa 185.17.215.32), etadm2.mdcr.cz (IP adresa 185.17.215.34) a dt.mdcr.cz (IP adresa 185.17.215.39) při ověřování kontrolním skenem dne 27. 8. 2020 stále podporovaly komunikaci protokolem TLS ve verzích 1.1 a 1.0, které již nejsou podporovány ze strany výrobců prohlížečů. Google ukončil z důvodu bezpečnosti podporu v rámci Chrome v dubnu 2020, Firefox a Safari v březnu 2020 a Microsoft s koncem prvního pololetí roku 2020.

Pracovní skupina INRFA dále vede úkol *Povolení TLS 1.3*. Servery crv.mdcr.cz (IP adresa 185.17.215.21), crr.mdcr.cz (IP adresa 185.17.215.58), sod.mdcr.cz (IP adresa 185.17.215.42), istp.mdcr.cz (IP adresa 185.17.214.147), rpsd.mdcr.cz (IP adresa 185.17.215.27), etesty2.mdcr.cz (IP adresa 185.17.215.32), etadm2.mdcr.cz (IP adresa 185.17.215.34) a dt.mdcr.cz (IP adresa 185.17.215.39) verzi 1.3 protokolu TLS k datu ověřování nepodporovaly, a to ani na testovacích prostředích.

Míra významnosti zjištění:	Střední
Identifikovaná rizika:	MD neprovozuje aplikace dle postupů stanovených BPI MD. Provoz nepodporovaných verzí komunikačních protokolů zvyšuje riziko úspěšného napadení aplikací MD v okamžiku případného kybernetického útoku. S ohledem na sdílenou infrastrukturu by pak mohly napadené aplikace posloužit jako vstupní brána do IS MD.

Doporučení:

O 110, O 160

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.

Stanoviska auditovaných subjektů:

Stanovisko O 110

Akce:

1. Zajistit vypnutí volatilních verzí TLS – souvisí se zabezpečením komunikace s tlustým klientem, RPSD a dalšími DSA (aktivita aktuálně probíhá)

Dočasně vyřešeno pomocí změny sady podporovaných šifer. Trvale bude řešeno povýšení verze operačního systému, programovacího jazyka a knihoven, a to v rámci chystané analýzy a následné úpravy celého systému.

Stanovisko O 160

IS CRŘ

Řešení TLS 1.3 je monitorováno ze strany PS CRŘ, přičemž O 160 očekává průběžné informování ze strany O 330, popř. PS INFRA.

IS DT

Přechod komunikace IS DT se třetími stranami s využitím protokolu TLS 1.2 a následné vypnutí nepodporovaných verzí protokolu TLS 1.0 a 1.1 je intenzivně řešen od konce roku 2019. Původně plánovaný termín nasazení do produkce byl do 31. 3. 2020. Termín byl odložen jednak z důvodů řešení administrativních náležitostí spojených s objednávkou rozvojových prací a naplněním požadavků Usnesení Vlády č. 86/2020, a dále z důvodu nepřipravenosti testovacího prostředí na straně MOVE-HUB jakožto provozovatele TACHONET. Všechny uvedené skutečnosti byly součástí podkladů předaných v rámci rozhovorů s auditorem.

Dané zjištění bude napraveno s nasazením rozvojových úprav IS DT, které je plánované nejpozději do 30. 11. 2020.

IS eTesty

Předmětná opatření jsou v současné době konzultována a realizována dodavatelem.

Reakce auditorů/Závěr:

V uvedených stanoviscích auditorský tým neidentifikoval důvody pro revizi zjištění.

Zjištění zůstává beze změny.

Číslo zjištění:	5
Název zjištění:	Nevhodné kombinace algoritmů dohod na klíči a šifrování klíčů

Popis zjištění:

Příloha č. 4 Pravidla pro provozovatele IS BPI MD, odkazuje v části V. Kryptografická opatření, kapitola 2 Symetrické algoritmy asymetrické algoritmy a hashovací funkce, na aktuální doporučení Národního úřadu pro kybernetickou a informační bezpečnost a nesoulad má být řízen formou výjimek v souladu s přílohou č. 6 Řízení výjimek BPI MD.

Servery crv.mdcr.cz (IP adresa 185.17.215.21), crr.mdcr.cz (IP adresa 185.17.215.58), sod.mdcr.cz (IP adresa 185.17.215.42), istp.mdcr.cz (IP adresa 185.17.214.147), rpsd.mdcr.cz (IP adresa 185.17.215.27), etesty2.mdcr.cz (IP adresa 185.17.215.32), etadm2.mdcr.cz (IP adresa 185.17.215.34) a dt.mdcr.cz (IP adresa 185.17.215.39) v rámci procesů dohod na klíči a šifrování klíčů používají AES v módu CBC – TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS a TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS.

Server dt.mdcr.cz (IP adresa 185.17.215.39) dále umožňuje použít AES v módu GCM resp. CBC – TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d), TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c), TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d), TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c), TLS_RSA_WITH_AES_256_CBC_SHA (0x35) a TLS_RSA_WITH_AES_128_CBC_SHA (0x2f).

Servery etesty2.mdcr.cz (IP adresa 185.17.215.32), etadm2.mdcr.cz (IP adresa 185.17.215.34) a dt.mdcr.cz (IP adresa 185.17.215.39) podporující komunikaci protokolem TLS v nepodporovaných verzích 1.1 a 1.0 (viz Zjištění č. 4) v rámci procesů dohod na klíči a šifrování klíčů používají AES v módu CBC s hašovací funkcí SHA – TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) s ECDH x25519 (ekvivalent 3072 bitů RSA) respektive ECDH secp384r1 (eq. 7680 bits RSA) FS. Server dt.mdcr.cz (IP adresa 185.17.215.39) dále umožňuje použít AES v módu CBC s hašovací funkcí SHA – TLS_RSA_WITH_AES_256_CBC_SHA (0x35) a TLS_RSA_WITH_AES_128_CBC_SHA (0x2f).

Z uvedeného vyplývá, že servery KII a VIS v rámci procesů dohod na klíči a šifrování klíčů používají algoritmus AES v režimu CBC, v některých případech i s hašovací funkcí SHA. Při použití algoritmu AES v režimu GCM není v některých případech serverem uplatněno nastavení dopředné bezpečnosti. Jinak řečeno, při komunikaci nepodporovanými protokoly nelze využít žádnou kombinaci algoritmů dohod na klíči a šifrování klíčů, kterou lze považovat za bezpečnou.

Míra významnosti zjištění:	Střední
Identifikovaná rizika:	MD neprovozuje aplikace dle postupů stanovených BPI MD. Nevhodné kombinace algoritmů dohod na klíči a šifrování klíčů zvyšují riziko úspěšného napadení aplikací MD v okamžiku případného kybernetického útoku. Využití hašovací funkce SHA není v souladu s platným doporučením Národního úřadu pro kybernetickou a informační bezpečnost.

Doporučení:

O 330

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.

Číslo zjištění:	6
Název zjištění:	Nesoulad požadavků na fyzickou bezpečnost

Popis zjištění:

BPI MD v části VIII. Fyzická bezpečnost odkazuje na pravidla, zásady a principy uvedené v platném znění Směrnice č. 1/2014 - Směrnice k zajištění bezpečnostní ochrany objektu Ministerstva dopravy. Pravidla stanovená pro objekt MD, nábřeží Ludvíka Svobody 12, za účelem zamezení neoprávněného vstupu, zamezení poškození informačních aktiv a zajištění ochrany informačních aktiv na úrovni objektů a v rámci objektů jsou dle směrnice platná pro veškeré lokality, budovy a místnosti, ve kterých jsou uložena nebo provozována informační aktiva. Ve směrnici č. 1/2014 není uveden požadavek na uzamčení rozvaděčů.

Požadavky na zajištění fyzické bezpečnosti informačních aktiv specifikuje příloha č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019, smlouvy 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. Smluvní ustanovení definuje požadavek na umístění hardware pro provoz infrastruktury do **uzamykatelných skříní s řízeným přístupem a s chráněnými přístupy ze všech stran**. Požadavek na uzamčení však není blíže specifikován.

Při fyzické obhlídce datového centra Chodov na adrese V lomech 2339/1 byly zamykatelné rozvaděče s hardware MD na sálech **v 3. NP uzamčeny**, rozvaděče na **sále v 1. NP** byly zamykatelné, avšak **uzamčeny nebyly**. Sály na 3. NP slouží k provozu serverů s možným přístupem pracovníků třetích stran, sál v 1. NP je provozován pouze pro potřeby zákazníků O2 a je přístupný pouze technikům O2. Předložený provozní řád datových center O2 povinnost uzamykat rozvaděče nijak neupravuje.

Jelikož je Služba provozu CRŘ – KL003, příloha č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019, smlouvy o Poskytování služeb provozu infrastruktury pro informační systémy Ministerstva dopravy, ev. č. S-8-330/2017, ze dne 16. 5. 2017, provozována pouze v rámci datového centra Nagano na adrese K Červenému dvoru 25/3156, ověření uzamčení rozvaděčů na místě auditorským týmem realizováno nebylo, a to s ohledem na plánovaný přesun služeb do nového datového centra Stodůlky. Dle sdělení pracovníků dodavatele ICZ a.s. na interview jsou rozvaděče uzamčeny a klíče mají k dispozici 2 administrátoři společnosti ICZ a.s. a stálá služba datového centra Nagano.

S ohledem na definované požadavky na zajištění fyzické bezpečnosti informačních aktiv nebylo porušení smluvních ustanovení ve smyslu přílohy č. 1 dodatku č. 2, č. j. 2/2017-330-SML/98, ze dne 27. 2. 2019 identifikováno. Efektivita

<table>
<tr><td colspan="2">opatření v oblasti fyzické bezpečnosti v podobě zamykatelných skříní je však v případě datového sálu v 1. NP de facto nulová.</td></tr>
<tr><td>Míra významnosti zjištění:</td><td>Nízká</td></tr>
<tr><td>Identifikovaná rizika:</td><td>MD neprovozuje aplikace dle postupů stanovených BPI MD.

Ustanovení BPI a smlouvy vyžadující konkrétní opatření v oblasti fyzické bezpečnosti jsou vynucena formálně. Praktické nevyužívání stanovených opatření snižuje výslednou míru zónové ochrany.</td></tr>
<tr><td colspan="2">Doporučení:

O 330

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.</td></tr>
</table>

5. ZÁVĚREČNÉ SDĚLENÍ

Zpráva o auditu kybernetické bezpečnosti č. 1/2020 byla vyhotovena na základě Návrhu Zprávy o auditu kybernetické bezpečnosti č. 1/2020, který byl rozeslán auditovaným subjektům dne 30. 9. 2020, a vyhodnocení stanovisek předložených auditovanými subjekty – Odborem silniční dopravy, Odborem provozu silničních vozidel a Odborem agend řidičů. Odbor ICT k Návrhu Zprávy o auditu kybernetické bezpečnosti č. 1/2020 písemné stanovisko nezaslal.

Stanoviska auditovaných subjektů jsou v plném znění uvedena v části 4. této Zprávy, společně s reakcí auditorů a závěrem, zda na základě stanovisek došlo k revizi zjištění a doporučení či nikoliv.

Auditorský tým vyjadřuje tímto své poděkování zástupcům auditovaných subjektů za jejich vstřícnost a příkladnou spolupráci při provádění auditu.

V Praze dne 12. listopadu 2020

Vedoucí auditorského týmu:

Za členy auditorského týmu:

Zpráva o auditu kybernetické bezpečnosti č. 1/2020 obsahuje 29 stran.